Overseas Development Institute

HPG Report

HUMANITARIAN POLICY GROUP

The Humanitarian Policy Group at the Overseas Development Institute is Europe's leading team of independent policy researchers dedicated to improving humanitarian policy and practice in response to conflict, instability and disasters.

Mainstreaming the Organisational Management of Safety and Security

A review of aid agency practices and a guide for management

By Koenraad Van Brabant

HPG Report 9
March 2001

Notes on the Author:

After a number of years managing humanitarian aid programmes in conflict prone areas, Koenraad Van Brabant joined the ODI as Coordinator of the Humanitarian Practice Network and as Research Fellow. Between 1998 and 2000 he did much work on security management, in the form of research, training, networking and advocacy. This latest critical review of management practices complements an earlier critical review of security training, and the authorship of a field manual on operational security management in violent environments.

Acknowledgements:

The author gratefully acknowledges financial support from the US Office for Foreign Disaster Assistance (OFDA), directly and through InterAction. This report does not necessarily reflect the views and opinions of OFDA, InterAction, or of any of the individuals or agencies consulted.

Thanks to Lucy Morris and Rebecca Lovelace at ODI for the formatting and production of this report and to Corwen McCutcheon for the copy-edit. Also to Lucy Brown at the American Red Cross for her assistance with the research and to John Cosgrave, Nick Leader and Sarah Longford for their useful feedback on an earlier draft.

Please send comments on this paper to:

HPG
Overseas Development Institute
111 Westminster Bridge Road
London
SE1 7JD
United Kingdom

Tel: +44 (0) 20 7922 0300
Fax: +44 (0) 20 7922 0399

Website: www.odi.org.uk/hpg
Email: hpgadmin@odi.org.uk

A copy of your comments will be sent to the author

ISBN: 0 85003 494 9

Contents

LIST OF BOXES

LIST OF FIGURES AND TABLES

Abstract

This report offers a comparative overview of recent aid agency attempts to strengthen the management of safety and security. It is based on consultation with 20 organisations, including NGOs, the Red Cross Movement and UN agencies.

It begins by clarifying the conceptual and practical similarities and differences between safety and security and then notes what triggers efforts to effect organisational improvements, as well as where resistance within an organisation may lie and why. It considers what different management approaches are in place, where agencies locate the safety and security expertise in headquarters and the sometimes difficult questions of clarity about authority, responsibility and lines of communication. It then reviews important management tools, such as fora in headquarters to discuss organisational safety and security management, a safety and security review, the development of a common security concept and a common understanding about possible security strategies, a safety and security policy, and questions of funding safety and security measures. It goes on with a detailed overview of various efforts to implement improvements, in operations in general and with regard to very specific threats, in personnel management in general, and with regard to staff competence development. There follows a look at relationships between aid agencies, and between aid agencies and other actors, such as the military, private security companies, embassies and the national authorities, particularly in the context of security management. The penultimate section offers an overview of the most important factors to inhibit or facilitate organisational improvements, together with more general organisational characteristics that may influence the ease with which these can be effected. It concludes with the suggestion that organisational improvements can usefully be directed and driven by a management plan. Such a management plan will be different for each organisation and vary according to the stage of development.

The report offers not only a management review, but also provides tools and arguments for managers to review rapidly where their organisation is, to orient improvements and to identify objectives.

Introduction

1. Who is this report for?

This report is first intended for senior management in aid organisations, as it discusses overall organisational responsibilities, practices, development and change. This includes executive directors or chief executive officers, and their deputies or vice-presidents, as well as heads of operations, human resources, medical or health, policy, fundraising and press and communication departments, divisions or units. Mid-level managers and security focal points in headquarters are also likely to find it useful. Others for whom it should be of value are change managers, consultants tasked with organisational reviews and training providers.

It will also be of strong interest to institutional donors. For those donors with operational activities in risk areas, such as Swiss Disaster Relief, the Swedish Rescue Teams, USAID's DART teams or the Crown Agents for the UK government, the report is also relevant, as they too have a moral and perhaps legal responsibility for people deployed in risk areas on their behalf. This is also true for aid administrations such as ECHO, that field 'consultants' or 'correspondents' in danger zones.

The management structures described and analysed here do not necessarily fit research organisations or university departments whose researchers and research assistants go regularly to risk areas, but the report should raise questions and stimulate reflection for them as well.

2. The contents of this report

The security of aid agency staff in recent years has been a growing concern for managers of aid organisations and their donors. This report offers a comparative overview of recent aid agency attempts to strengthen the management of safety and security. The 20 agencies consulted included US and European NGOs, the ICRC and the IFRC and three UN agencies.

Part 1 presents an overview of the key managerial issues that need to be addressed. It is in a way an 'executive summary' of the main report. I considered producing an 'executive summary' of two to three pages, but so much condensing of the main report would have left the reader with meaningless simplifications and major omissions. Part 2 is the main report; it provides more, often important, detail and especially examines and develops the arguments for and against certain practices. It concludes with the suggestion that organisational improvements can usefully be directed and driven by a management plan. Such a management plan will be different for each organisation and vary according to the stage of development.

One starting-point for such an exercise is a thorough analysis of where an organisation is: for that purpose the report also offers a comprehensive and detailed 'question sheet', to help managers take stock and explore the arguments (Annex 4). Annex 5 presents an outline of what could be the desired end-state of organisational change, that is a profile of an aid organisation that is highly competent at risk management.

3. How can this report be used ?

On one level this report is a mapping exercise: it provides a critical, but not judgmental, comparative review of how far 20 aid organisations perceive themselves to be with regard to safety and security management. Because many of them were selected on the basis that it was known they had been actively concerned with this issue in recent years, it can be fairly confidently assumed that the resulting picture represents the current 'state of the art' for safety and security management in the sector. As such it provides a benchmark for those consulted as well as for other aid agencies.

This report, however, does more than take stock. Through presenting ideas, approaches and experiences of a range of agencies, asking critical questions and exploring and developing the arguments, it also intends to be of practical use to organisational managers. It can stimulate discussion, inspire a quick or more thorough review of where an individual organisation is and be of help developing a management plan to strengthen safety and security in a more systematic manner.

It is also possible to use, or refer back to, certain parts of the main report that focus on specific topics. But in so doing, the main message - to develop the organisational competence in a systematic rather than an *ad-hoc* manner - should not be forgotten.

4. What this report does not address

The report presents a management review and offers tools for organisational managers.

It does not contain an exhaustive examination of the broader trends and the policy and political environments that have brought 'security' higher on the agenda in the aid world, and the particular but sometimes contested, interpretations of roles and responsibilities within the larger conglomerate of the aid world that national authorities, different donors and operational agencies may adopt.

Although this report reviews current practices in the organisational management of some threats, it does not deal with all those possible. It also offers no detailed guidance on

the operational management of security in danger zones. That guidance is contained in the *Field Handbook on Operational Security Management in Violent Environments* (Van Brabant, 2000), that inspired many of the questions explored in this research.

The emphasis on aid agency management should not distract from the fact that national authorities have the primary responsibility for the security of people in their territory, a responsibility that is enshrined in various legal instruments.

Abbreviations

FSO	Field safety or field security officer
GEOM	Geographical manager at headquarters (desk officer/regional director)
HoD	Head of delegation (field coordinator/country representative/country director)
HQ	Headquarters
HR	Human resources department (personnel department)
SFP	Security focal point (security officer) at headquarters

Mainstreaming Safety and Security Management: A Summary

The security of aid-agency staff is of growing concern to managers of aid organisations and their donors. The fact that agencies increasingly find themselves working in violent environments, and particularly the perception that they are being targeted, has given rise to a range of internal measures, as well as inter-agency initiatives. After an initial emphasis on security (acts of violence), staff safety (accidents and health) is attracting renewed attention.

Yet there is confusion between security management, and safety management. Organisations are responsible for the safety and security of their staff. Both can be subsumed under the concept of 'risk management'. But while there is significant overlap between measures to improve safety and measures to improve security, the two are not identical, and focusing on one at the expense of the other leaves dangerous omissions.

In a number of aid organisations, improvements are being delayed by arguments against prioritising and investing in better safety and security management. The most common arguments are:

- 'we are not in the emergency or life-saving business';
- 'we haven't had any deaths in the organisation';
- 'risk is an unavoidable part of our work'; and
- 'we have been managing risk for decades with existing tools and competences, so there is no need for additional or new measures'.

These arguments reveal dangerous assumptions:

- that the level of risk has remained the same over the past three or four decades;
- that the only risk that counts is that to the life of staff (for which, perhaps, read international staff);
- that no deaths in the past guarantees none in the future;
- that risk is only high in actively violent conflict zones, and therefore mainly concerns agencies with a life-saving mandate; and
- that risk cannot be reduced through individual and organisational measures.

These assumptions go against the available evidence and analysis, which indicate that incidents are becoming more frequent, with crime now accounting for perhaps 50 per cent of all incidents; that more agencies are working in danger zones; and that the overall respect for them, and therefore for the 'immunity' of their staff, has significantly declined.

Among field staff, there is also a concern that giving priority to their safety and security somehow conflicts with the organisation's fundamental mission, which is to help people in need. There is indeed an incompressible element of risk in humanitarian aid work, but good security management is also a tool to help agencies enter and remain in danger zones. The loss of staff and assets, either through accident or incident, actually makes it more difficult for an agency to carry out its fundamental task.

Within organisations, change appears to happen in three broad ways:

- change driven by mid-level managers;
- change driven by top management; and
- change driven by a strong commitment to the safety and security of staff by both top and mid-level management.

Organisations which are generally committed to safety and security management tend to have a culture of care for staff, a commitment to competence and professionalism and a commitment to being a learning organisation. The importance of the attitude of the director of the organisation cannot be underestimated: 'safety and security does not start with the type of staff member you recruit, it starts with the type of Chief Executive Officer you recruit', as one aid worker put it.

Management structures

Three types of managerial set-up for strengthening safety and security are in vogue:

a) The management line model, where safety and security is located, with other general management responsibilities, within the operational line management between headquarters and the field. A problem for line managers here is lack of time and, sometimes, of sufficient competence.

b) The specialist security officer model, where one or more such posts are created at headquarters and in the field, often outside of, and subordinate to, the line management. A frequent problem here is the lack of interest and/or competence among line managers, who can ignore or override the 'advice' of a security officer.

c) The security advisor model, where the responsibility for security management lies within the management line, but there are one or more security advisors at headquarters, who support the organisation as a whole, and specific field offices.

Several agencies have designated staff as their 'security focal point'. In practice, this can cover different roles: the specialist security officer or the security advisor can be full time, but

also can be a senior line manager, who ensures that security remains on the agenda of top-level managers, and who, as time allows, directs organisational efforts to improve safety and security management.

Security expertise in headquarters is usually located in the operations department, although in multi-mandate agencies it can be found in the emergencies or disaster response departments. This should be questioned. Safety and security risks may be highest in conflict areas, but they are also present in 'developmental' situations. Landmines and unexploded ordnance, for example, can remain a threat decades after a conflict has ended, and crime often poses more of a threat in so-called 'stable' situations. A health and safety officer may complement security expertise. This post tends to be located in the human resources department, although some put this post, and in-house stress councillors, in operations. The human resources department plays an important role in ensuring that safety and security standards in the organisation are maintained. It thus needs to be actively involved in safety and security management.

Good safety and security management requires clarity about authority and responsibility, lines of communication and decision-making. Good practice holds that authority and responsibility are vested in line managers, and that safety and security are managed 'close to the ground'. However, decentralised organisations risk losing overall consistency, and the checks and balances that headquarters provide. At field level, safety- and security-related tasks tend to be delegated to other staff, notably logisticians, field security officers and/or administrators. This should not result in an abdication of responsibility by the head of the field operations. The more 'focal points' on safety and security there are in headquarters and the field, the more important it becomes to maintain streamlined communications, so that managers can retain overview and responsibility for decisions.

Management tools

Making significant improvements in organisational safety and security management requires one or more fora at headquarters where discussions can take place. An ad hoc working group can do the job, but the question remains: what happens when it dissolves? That problem can be overcome by a standing working group to drive forward initiatives and monitor their implementation. For both mechanisms to be effective, senior management needs to be represented.

Organisations that have achieved a strong safety and security culture can rely on regular meetings of their operations and senior management teams, creating ad hoc working groups as the need arises.

A useful tool is a safety and security review. This can be conducted by staff, or by outsiders. It will, however, only be effective if top management follows up on its recommendations. An important precondition for improved security management is clarifying what security concept is appropriate. Not recommended are concepts of 'corporate security' with 'VIP protection', nor a narrow 'procedural-technical' concept that emphasises protective procedures and devices. What is recommended is a multi-dimensional security concept, that brings into play the values and principles of the organisation, its mandate and mission, contextual analysis and scenario monitoring, the organisation's position in relation to a multitude of actors in a particular context, the nature and design of field-level programmes and the way the organisation manages its staff. An understanding of the range of security strategies available needs to be developed. These encompass acceptance, protection and deterrence. Choosing the most appropriate mix of strategies depends on the threats and risks of a particular context, not a normative preference for one over the other.

Few agencies currently have a safety and security policy. It is possible to develop a policy relating specifically to security and another one to safety, or to integrate both. The value of such a policy is that it makes safety and security management a corporate responsibility, rather than an operational issue. It then obliges management to act, and legitimises the allocation of staff time and other resources. An argument in some organisations against developing much written policy is that it creates more bureaucracy. This is a risk, but there are nonetheless powerful arguments in favour of putting things on paper. Apart from legitimising management decisions and resource allocations, it also reduces inconsistency in organisational practice.

A key management question will always be finance: insurance, equipment and infrastructure upgrading all cost money, as do training and salaries. Until recently, the most common and largest expenditures on security were probably related to communications equipment and training. For many organisations, new expenditure requirements are now emerging. One is for increased site protection, due to a rise in crime. A second is the need for pre-positioned security equipment, to be used in initial risk assessments and in the deployment of the first wave of emergency-response personnel. Only very few organisations have reached the point where safety and security is fully written into operational budgets. Even then, some reserve funds probably have to be kept available centrally, to cover unexpected and non-budgeted requirements. New headquarters positions dedicated to security can be difficult to fund, particularly for agencies which depend on institutional donor funding. Generally, agencies feel that donors are receptive to funding security requirements, although there is concern that donors might use security-linked funding to influence where agencies deploy.

Operational reinforcements

The need to carry out risk assessments as part of the very first needs assessment, prior to going into or returning to a danger zone, is gradually being recognised. This marks a

slow change in organisational culture, with risk awareness and management introducing caution into a sector with a competitive and action-oriented mentality.

Several organisations see the pursuit of neutrality in a fragmented and conflictual environment as part of an acceptance strategy, and therefore part of a security strategy. At the same time, there is unease about neutrality, which as a principle might not sit well with other values, such as solidarity and social justice. It is also arguable whether neutrality can be achieved in practice, and impartiality might be a more realistic objective. Agencies invoking neutrality need to clarify for their own staff what it means in practice.

The security plan has historically been the pillar of many agencies' security management. In practice, its production is often an administrative requirement, and the plan remains a 'dead' document. Having identified the problem, more agencies are now developing guidelines for security planning against a generic template that needs to be adapted locally, putting more emphasis on the planning process and on a team approach. Those most advanced in security management see the security plan only as one tool among others. Maintaining alertness, active monitoring of the environment, scenario thinking, incident analysis, and strengthening awareness, competence and discipline are other important tools. The emphasis is on a management plan for security, rather than on a security plan.

Having headquarters review the security plans developed by the field, and prompting field managers to regularly review them, is a common mechanism of quality control. Field visits by a security advisor or a desk manager from headquarters, as well as in-country training courses, can be opportunities for a more in-depth review of the risk assessment and the measures for risk reduction. The most formal quality control would be an evaluative 'security audit'. Depending on the organisational culture and the individuals involved, this will be experienced as a policing action or as a learning opportunity. Security management could also be included in the terms of reference of a programme evaluation.

In only a few agencies are headquarters staff confident that they know about almost all incidents. The most common disincentives to incident reporting include concern about subsequent headquarters interference in the programme, or about potential damage to career prospects if an incident is seen as a management failure. Incident analysis could also be improved, as could the sharing of incident reports between agencies.

For years, telecommunications have been the main security technology. However, agencies working in battlefield zones may need the technical skill to properly construct blastwalls and bomb shelters. With the rise in crime, including violent crime, in many countries, site protection is becoming of greater concern. Many experienced logisticians and some security officers do not have sufficient technical knowledge of (new) weapons threats, for example cluster bombs and depleted uranium, or the protective devices against them. This may imply additional training, and knowledge and skill development for selected staff members.

Safety and security measures reduce risk, but cannot fully eliminate it. 'Crises' may therefore occur. Some organisations have thought through their crisis preparedness, but others have not identified who would or should participate in a crisis-management team at headquarters, or how certain types of crisis should be managed. Steps towards better crisis preparedness include: clear definition of what a 'crisis' is; 24-hour communications with headquarters through a system of duty officers who are clear about the parameters of their decision-making authority; the identification of core members of a crisis-management team (with identified substitutes in case a member is not available); and training.

There are generic characteristics to crisis management, but there are also aspects which are specific to the type of incident. Evacuation is one example. The risk of kidnapping has drawn much attention, and several agencies have obtained outside advice on how best to manage such situations. By contrast, sexual assault and rape remain largely neglected areas, although there must be as many, if not more, such incidents. There is significant confusion about how to manage this threat, confusion which is not helped by treating the matter as taboo or claiming that nothing can be done about it.

Where the risk is beginning to be acknowledged, management responses frequently approach it in the context of sexual harassment, or as one type of traumatic incident for which counselling is offered. This is grossly inadequate. At a policy level, sexual harassment does not address the risk of rape by outsiders to the organisation. There is also a need to disentangle the problematic relationship between security and gender policy, whereby withdrawing women from high-risk zones is seen as going against the policy. This may not be acceptable when reflecting a general paternalistic attitude, but it is legitimate when based on a detailed risk and vulnerability assessment. Finally, protecting the victim's confidentiality needs to be balanced with the need to alert others to the existence of a threat. In terms of practical management, field managers need guidance on immediate rape response, which will have to take place before any professional post-traumatic counselling can be mobilised.

Concerning safety risks, a general weakness is likely to be in preparing staff for context-specific threats, such as operating in jungle and desert areas, high mountains with heavy snowfall, or in situations where they often have to make use of local transport with low safety standards. Safe sex, to protect from sexually transmitted diseases, is explicitly addressed by many agencies. Several organisations ensure that condoms are available to national and

international staff in the field, and can be obtained discreetly. For some religious organisations, this proves impossible, and they limit themselves to advising staff to use condoms.

Improving personnel management

Aid organisations are beginning to more formally acknowledge their responsibility for the safety and security of their staff. Spelling out the detailed commitments of the organisation to its staff, particularly concerning kidnapping, sexual aggression, or disability as a result of an accident or incident, will increase staff trust and loyalty. Attention in any case must be paid to the evolving legal requirements of employers, and to national legislation relevant to national staff. It is doubtful that making staff sign a statement that they will not hold any claims against the organisation in case of incident or accident is morally and legally defensible. Few organisations have faced court cases brought by former staff or their relatives, but this is likely to change. Providing comprehensive insurance, including war risks and malicious act insurance, has become an essential requirement for many deployments. Detailed attention is needed as to whether staff with different contractual statuses are covered, whether coverage is adequate in the case of permanent disability, for example, and whether there are exclusion clauses in the coverage. This requires legal expertise.

At the same time, some organisations are also clarifying their expectations of individual staff members. In principle, staff can refuse to be deployed in a high-risk zone, but doing so repeatedly would suggest that the individual and the organisation should perhaps part ways.

Organisations are also increasingly stressing that observing security rules is mandatory, and that breaching them can lead to disciplinary action, including repatriation. Several agencies have clarified that staff members need to behave responsibly and respectfully at all times, not just during office hours. Personal behaviour can put staff at risk, or may damage an organisation's image and reputation. Some organisations are formulating a 'code of personal behaviour' document.

Attitudes to risk and risk management can be tested in the recruitment process, including for senior staff. Agency policies, practices and expectations can also be addressed in an induction/orientation course. Pre-departure briefings and in-country arrival briefings for international staff should cover context, the general pattern of threats and risks and the risk-reduction measures in place. Some agencies are open about the risks that staff members may face. At any stage in the assignment, the staff member can withdraw if she or he feels that the risk is more than can be coped with.

Post-deployment or end-of-contract debriefings, for national as well as international staff, are an opportunity to check the individual's well-being, and to gain feedback on the organisational management of risk.

Many surveys confirm that stress is a major staff concern. However, the organisational emphasis is often on post-traumatic or critical-incident related stress, rather than the less visible cumulative stress which can lead to 'burn-out'. There is also very limited awareness of, let alone attention to, significant cultural differences in how stress is experienced, and in responses to it.

Organisations have been mobilising competence on stress management in a variety of ways. These range from engaging professional consultants, raising awareness and giving practical tips to managers, to training in-house volunteers, based in headquarters or in the field, as stress monitors and/or providers of 'emotional first aid'. Agencies that regularly work in high-risk zones have often established a relationship with an external mental-health centre, where staff can get confidential professional assistance. In principle, agencies also want to take stress levels into account when deciding whether to redeploy staff. In practice, however, this often conflicts with the need for experienced staff who know the agency well.

More difficult is the fact that the safety and security of national staff in general remains a painful weakness; there is even resistance to facing the issue. Clarity of thinking is not helped by the automatic association with evacuation. This can make agencies overlook the fact that national staff also face health and safety hazards, and can be at risk from landmines, armed robbery, ambush, hostage-taking or sexual assault. Given that the global trend in staffing is for more national and less international staff, a change in attitude and more constructive thinking are urgently required. More progressive practices being adopted include more detailed vulnerability and risk analysis, differentiating between international and national staff and categories of national staff; insurance cover and training opportunities for national staff; and the articulation of basic policy principles that confirm the responsibility of the organisation to care for their national staff. Some organisations also offer social benefits for national staff who suffer accident or incident.

Developing in-house competence

This is a crucial issue, and it is important not to get distracted by the question of whether you need to recruit security officers with a 'professional' security background (i.e., ex-military or ex-police). The UN makes this a formal requirement, but some NGO personnel have been sceptical of this, if not outright critical. But the question misses the point. The real issues are:

- what range of competences is required for safety and security management?;
- does a person understand the differences between the major security strategies of acceptance, protection and
- deterrence?; and
- what specific competencies are most needed in a security officer in a given context?

Comprehensive safety and security management requires diverse knowledge and skills, including practical, technical and interpersonal skills, gender and cultural sensitivity and some anthropological understanding, the ability to carry out political analysis, and leadership qualities. Few individuals are likely to be equally knowledgeable and skilled in all of these aspects. The focus should not be directed at someone's background, but at his or her skill profile. Organisations that have embedded competence in line management have not seen the need to throw out all their operational managers and replace them with ex-military personnel. Automatically turning to 'ex-military' and 'ex-police' also reflects a mind-set that sees security as a specialist - and mostly male - domain. This is mistaken. Refreshingly, some agencies have female security advisors. Lastly, selected national staff could be given responsibilities for security management.

Training courses are the most commonly-used formal tool for developing competence (learning-by-doing is not a satisfactory approach, since it contains too great an element of unnecessary trial-and-error). Several organisations have availed themselves of external training opportunities, while a few have developed in-house training, on their own or within their 'family network'. There is now broad consensus among agencies that the priority is not awareness, but management training. Underlying this is an admission, sometimes unspoken and even unrecognised, that 'field-experience' provides fertile ground, but does not automatically and by itself mean 'full competence'.

Making significant organisational progress on safety and security management also requires developing a 'critical mass' of competent staff. The problem is that many managers do not get or find the time, or do not have enough motivation, to avail themselves of such training. For people to make use of training, they need to be able to put it into practice in their daily work. Investing in safety and security training will not pay off unless it is part of an organisation's wider development. An in-house 'training of trainers' approach tends not to work, unless these people are released from their normal duties and deployed in a small team to train staff in various field settings.

A key management question will be who needs to be trained on what, and to what level of competence, and who needs to be trained first. The time is not always taken to do this analysis, which is necessary to develop a targeted training plan. But training need not be the only tool: bringing in a mentoring function in one's management style, and taking time to discuss with staff the analysis, principles and logic that underlie approaches and decisions, creates effective on-the-job learning opportunities. At the same time, interactive and distance-learning materials are also being developed.

Safety and security resource and reference documents are the second major tool. In and between agencies, there is a vast amount of documents on this topic. While this indicates that agencies take it seriously, there are sometimes serious weaknesses that require management attention. Reference materials on certain topics, notably kidnapping, hostage-taking, rape response and stress management, are sometimes copied from literature developed in Western countries, and thus may not be appropriate for the settings aid agencies work in, and for all types of aid-agency staff.

It is not always clear for whom the documents were written: there is often a blurring between guidance for all field-based staff, and that for managers in the field. No materials seem to take account of the specifics of distance-management between headquarters and the field, or between a country office in a capital and operational bases deep in the field. Much documentation also fails to distinguish between preventive measures, incident survival and immediate incident or crisis response. Organisations differ in where they locate their safety and security information: in a personnel manual, an emergency-response manual, or a stand-alone document. Finally, there seems to be little understanding or appreciation of the importance of proper editing and lay-out, to make a document attractive and user-friendly. This may incur extra cost, but greatly increases the likelihood that it will be used.

Having written resources at hand does not, however, guarantee 'competence'. Making staff sign a paper that they have 'read and understood' the documents given to them may reduce the organisation's liability, but is hardly an effective way of helping staff to absorb the content and the logic behind these texts.

Agency autonomy: yes, but not to the bitter end

There is a fair degree of inter-dependence between agencies at field level. There is also significant scope for more inter-agency collaboration to develop greater competence in safety and security management. Yet the most emphatic message from aid organisations is that they insist on retaining full autonomy. This is legitimate inasmuch as agencies have formal responsibility for staff, but it should not blind people to areas where collaboration is possible, beneficial, and even required.

When it comes to safety and security, there are a variety of interactions between NGOs, some of them formal within 'family networks' or specific 'projects', others informal and more dependent on individual networks. Staff safety and security can become a point of concern and debate between organisations, when there are 'secondments' of staff from one to the other, and around 'joint operations/joint offices'. In principle, the responsibility for safety and security management lies with the operational partner or the 'lead agency'. But complications can arise when the agency that seconded staff, or is not the lead agency, is not comfortable with the quality of safety and security management of the operator or lead agency.

There is a formal arrangement between UN agencies, with UNSECOORD in New York nominating the Designated Official responsible for the security management of all UN staff in a particular country. For some years, the UN has also offered a framework Memorandum of Understanding to implementing partners, typically NGOs, that would part-formalise their relationship with regard to security. Most NGOs by and large refuse it. Although in times of crisis there tends to be great solidarity and mutual cooperation, there are also strongly-held and critical views within the UN and among NGOs about the quality of each other's security management. As long as the respective agencies avoid frank discussions around these issues and refuse to accept a need for changes in organisational cultures and practices on all sides, more serious and effective collaboration is not likely.

Although international agencies often work with and through national or local governmental or non-governmental partners, when it comes to safety and security management this relationship has yet to receive much focused attention. Attitudes range from 'this is not our concern' to 'a genuine partnership requires that we allow them to pursue their own strategies and we are prepared to offer them capacity-building support'. The issue is certainly worth thinking through for each given situation. Minimally, both local partners and international agencies should ask whether the other party to the 'contract' or 'partnership' is creating risks for them.

Many civilian aid agencies have used, or have had to use, the military for security. Several are uneasy about relating to the military in general, but few seem to have developed useful policy guidelines. It does not seem productive to pursue an answer about 'aid agency-military relationships' in general terms, beyond some basic principles. A more operationally-useful approach might be to ask what form of relationship can be considered with what military, under which conditions and for which particular tasks. A similar state of affairs seems to characterise the question of the relationship between aid organisations and private security companies. Again, many agencies have used local or international private security companies, but few seem to have useful policy guidelines. Attitudes range from 'in principle we don't use them' to 'this is a free-market economy, is this an issue?'. At stake are questions of principle, context, choice and management. These could usefully be thought through, to inform some policy guidelines.

If not enquired about, embassies would not normally arise when aid agencies describe their security management. Embassies appear not to be commonly-used as a useful access route to national authorities. Clearly, from a legal/formal point of view, the national authorities are responsible for the security of all those on their territory. The UN and the ICRC enjoy certain special 'privileges and immunities'. The 'legal protection' of staff of other aid organisations is more vague, and established more through association with, or by extension from, the ICRC and the UN. Most other aid organisations do not pursue greater security through more explicit protection in international legal frameworks. The relationship with national and local authorities, especially in conflict zones, can be complex and sensitive. Few agencies seem to offer their field managers any guidance on how to deal with national authorities.

Factors helping or hindering organisational change

There is strong convergence of opinion over those factors that make improving safety and security management more difficult, and those that make it easier. The most important inhibitors are:

- lack of interest and commitment from top managers;
- an organisational culture with either excessive voluntarism or excessive bureaucracy;
- excessive operationality, with nothing in writing;
- a competitive orientation that encourages risk-taking behaviour, or a self-congratulatory attitude that disregards failures and weaknesses;
- excessive centralisation or decentralisation in agency structure;
- a shortage of expertise, or its misuse;
- instability in the organisation or the team;
- excessive workloads; and
- complacency because few staff and managers are confronted with high-risk situations.

Facilitating factors include:

- active interest and commitment from top management;
- an organisational culture of care for staff, support for learning and attention to conditions on the ground;
- an organisational structure without excessive layers of management;
- effective fora for discussion, policy development and decision-making;
- the availability of staff that can stand back from day-to-day pressures and reflect and think strategically;
- internal triggers such as a dramatic incident or a safety and/or security review; and
- external pressure from the media and evolving legislation, as well as opportunities such as inter-agency developments of resources and benchmarks.

The size of the organisation, and whether it is faith-based, seems to have little influence. By contrast, the mandate and funding base, layers of management and 'change fatigue' (ie, the impact on staff motivation and organisational efficiency) have a strong influence, either positive or negative. Working in a 'family network', working with local partners, and decentralisation can complicate efforts to strengthen safety and security management, depending on how these general characteristics are managed.

Improving policy and practice: a management plan for change

Very few agencies seem to have developed a management plan to strengthen safety and security management. This may not be necessary once there is strong organisational awareness and competence, but may be a useful tool to drive a 'qualitative jump' at crucial moments in early organisational development. A management plan sets out concrete objectives that the organisation wants to achieve within a defined time-frame. It sets priorities and becomes the reference-point for designating responsibilities and allocating staff and financial resources. It will also be the reference for monitoring progress. Ideally, a management plan is based on analysis and objective-setting, rather than the availability of a given resource. Developing a management plan is not easy, but the exercise can be an important step in generating organisational commitment and momentum.

Mainstreaming Safety and Security Management: A Management Review

Chapter 1
Why this research?

In recent years the security of staff, especially when operating in violent environments, has become an increasing concern for operational aid agencies and their donors alike. Individual aid workers are concerned about stress, serious injury and even loss of life or limb. Senior agency managers may have concerns beyond the well-being of their staff: including legal and financial liabilities as employers, and the impact of a serious security incident on their fundraising and recruitment capabilities. Many aid agencies have been putting in place initiatives to improve the security of their staff (and assets). But different initiatives and efforts, such as agency-specific guidelines or manuals, security training, the creation of a security officer post, training of staff in post-traumatic stress counselling, have been introduced in a rather *ad hoc* manner.

A major development in the past few years has been the collective work on identifying good practices for the management of security at field level. This has generated a security management training curriculum and been consolidated in a comprehensive field manual (Van Brabant, 2000). But good practice at field level requires organisational support. This report now provides an analytical overview of current organisational approaches and practices, with a critical appreciation of their effectiveness, derived from the perceptions of HQ-based staff.

In general three major questions were explored:

- What has your organisation being doing to strengthen its management of safety and security. How well are good practices adhered to and why or why not?
- What have proven to be catalysing and facilitating factors to strengthen safety and security management, and what have been more inhibiting factors or obstructive?
- What general characteristics of your organisation influence the ease or difficulty with which you can effect and maintain good practice in safety and security management?

The research underpinning this report was conducted between May and August 2000; within this period 20 agencies were consulted. It is fair to say, however, that in a broader sense, the research draws on three years of collaborative work involving many people in different agencies identifying good practice for field-level security management. The insights and understanding developed in the course of that earlier work about requirements at field level, have informed the detailed questions pursued in this round of consultation.

It must be made clear that this research did not constitute an evaluation of whether agency practice fully matched their verbal assertions or were found wanting. This was not its intent and the methodology used would not be sufficiently robust for such an evaluation. It is clear that all aid agencies are on a learning curve. Some have gone further than others, but the main aim of this research and report is to facilitate learning from the collective experience so far. The report is intended for consideration by other agencies than those consulted, some of which may not yet be so advanced. More detail on the methodology can be found in Annex 2.

The report is written in a critical mode, but this should not be taken to imply an overall negative judgement about the state of the art. Most ideas for good practice come from agency realities. But as the report indicates, there are still important areas where safety and security management can be clarified and strengthened. Its tone is argumentative, to provoke thought and reflection.

A conscious choice has been made to retain the sometimes colourful language of informal discussions as it tends to be more precise - rather than translate into 'diplomese'. No offence is intended.

Chapter 2
Strengthening safety and security

2.1 Safety and security

A conceptual distinction can be made between 'safety' and 'security', whereby the former refers to accidents and diseases, while the latter refers to acts of violence. There are two schools of thought: those agencies that quite explicitly make the conceptual distinction, and those that equally explicitly do not want to do so.

The debate about whether safety or security constitutes the highest risk (in terms of probability) - in layman's terms the question of whether more staff get killed in car accidents than by bullets- is misleading if it suggests that the management of one group of risks should have priority over the other.

One can argue that the distinction between safety and security is artificial and that both need to be integrated:

- Morally and legally, organisations as employers should be equally concerned about protecting their staff from safety *and* from security risks.
- In practice, safe driving, keeping vehicles in good working order, first-aid expertise and medivac facilities, and fire hazard prevention and preparedness are essential requirements for operating in a violent environment with risks of arson or ambush on the road, getting caught in the crossfire or seriously injured by a landmine.

At the same time, while the measures and competences to manage safety are necessary, they are insufficient to manage all the risks and realities of violence, which carry additional complexities. Competence and measures to reduce the risks and impacts of violence can include most safety risks, but are likely to overlook some others (for example, the risk of sexually transmitted diseases from unprotected sex). In short, there is considerable complementarity and overlap between both areas, but they are not identical.

The question is how to translate this into management responsibilities and competence development:

- As the safety and security of staff are a general organisational responsibility, they are components of the whole field of personnel management. Inasmuch as operations-related line managers (desk officers at HQ and heads of delegation) count personnel management among their responsibilities, this must include both safety and security.

- At HQ level, however, several agencies have different focal points or locations: safety tends to be primarily located within the human resources department, where a health and safety officer is likely to be located. Medical agencies tend to have a (public) health department at HQ, where the organisational concern for specifically staff health is likely to be found. Security is usually located within the emergency/disasters/operations department or unit, where most security focal points or security officers at HQ are put.

- When a head of delegation (HoD) in the field delegates responsibilities, or shares them out in a larger team, the logistics officer is most likely to be assigned security (logistics already involves vehicle and movement management, compound and warehouse management), whereas a medical officer (common in medical agencies) and/or administrator (with general personnel management responsibilities) are more likely to be assigned safety (especially health).

Among agencies that in recent years most actively have strengthened their overall safety and security management, security received priority attention, probably because of the urgent need to catch up with changing realities on the ground. Safety is now attracting renewed attention as an organisational attention point as well as in training efforts. The over-arching concept of risk management and talking about safety and security, or using either term to refer to both, then becomes a way of signalling that safety cannot be overlooked and exclusive attention paid to security.

2.2 A range of measures

The growing concern for the safety and security of aid agency personnel in recent years has spawned a variety of actions and initiatives within and between aid agencies. Some of the visible expressions of this, among others, are the development of internal agency guidelines or manuals (sometimes published and more widely available), the identification of a security focal point and/or the recruitment of designated security officers at HQ and/or field level, the development and delivery of training (in-house or inter-agency), the allocation of more funding for security-related expenses, the use of internal or external expertise to conduct organisation-wide or country specific security reviews. Aid agencies have also created or used various events, such as seminars, conferences and UN Security Council meetings, to draw attention to what is perceived as growing risk to their staff (for example Bertini 2000, UN 2000).

2.3 Triggers

Not surprisingly the experience of working in acutely dangerous situations, and particularly the direct experience

of dramatic, fatal or potentially fatal incidents acts as a major stimulus for the strengthening of security management in the organisation. Examples of this are Somalia in the early 1990s; the Great Lakes since 1994; Chechnya in 1996-1997, and in 1999 the (contemplated) return to the northern Caucasus; Sierra Leone since the mid-1990s; and most recently, the murder of three UN staff members in West Timor. Crucial here has not been simply the frequency or seriousness of the incidents, but the perception that aid agencies were being targeted.

The types of incident that appear to leave the deepest mark are kidnappings and hostage taking, the assassination of a staff member, and plane crashes with loss of several lives. Serious incidents drive a message home: 'Our organisation is not bullet-proof.' The loss of life or limb on a landmine seems to have less of a catalysing effect, the rape of a staff member little if any.

Although seldom explicitly stated, it is hard to avoid the impression that an incident affecting national staff has far less strong organisational repercussions than one affecting a (white/Western) international staff member.

Developing legislation with regard to the responsibilities and liabilities of organisations as employers is recognised as relevant, but does not appear to be an equally strong trigger. In some organisations there may be some doubt whether they are equally legally liable for international staff deployed abroad, especially when these have signed a waiver of their right to claim compensation from their employer as part of their contract.

2.4 Supporting factors

For several agencies consulted, the People-in-Aid project has and continues to be a supporting factor in making organisational improvements around safety and security management. This certainly applies to most of those who are formally piloting the Code of Conduct, but also to others who have made good use of some of the reports and courses on offer from the People-in-Aid project.

The People-in-Aid project originated in 1996 from a perceived concern about the security of aid personnel. In other words, its Principle 7 ('We take all reasonable steps to ensure staff security and well-being.') was in fact the starting-point. The other principles (one to six) were developed as prerequisites for improvements to be made with regard to principle 7. A first, voluntary, review in 1999 among piloting agencies, highlighted the fact that agencies had not yet fully taken up safety and security as a corporate responsibility, and needed to make more specific progress on improving practices in this regard (People in Aid 1999). The review stimulated more focused efforts as follow-up.

There are some aid agencies that in recent times have been expressing a fairly general scepticism towards a growing number of initiatives to do with codes and standards, which may affect their attitude to the People-in-Aid project. But People in Aid is not about a code that agencies must sign up and then adhere to. The People-in-Aid project, and its code, intends to be a tool and a support, to focus attention, provide a benchmark and a review opportunity through a social audit. According to its project manager, agencies take it up *because* they are already committed to change and improvement.

Another major supporting factor has been the development and availability of more training courses on security awareness and security management, notably the training curriculum developed and piloted under OFDA/InterAction auspices and now delivered primarily by RedR.

Conferences and seminars or other projects around security, were not mentioned as triggers or supporting factors.

The fact that more agency staff are expressing concern for security is probably more a supporting than a trigger factor.

BOX 1: The available evidence and analysis

This indicates that:

- The number of incidents affecting aid agencies has risen significantly since the end of the Cold War era and continues to rise.
- Agency practices have changed and that more and more agencies in recent years enter into high-risk danger zones, whereas before few besides the ICRC did so.
- Crime now accounts for perhaps 50% of all incidents, and is a risk in many settings where no active 'war-type' conflict is being fought out, thus threatening also staff from organisations with a more developmental mandate.
- Overall respect for aid agencies and therefore for the 'immunity' of its staff has significantly decreased in recent years, and that on a number of occasions aid agencies have been targeted for political reasons or because they are a 'soft and wealthy' target.
- The number of deaths among international staff is significantly fewer than that among national staff, and that the overall trend of less international and more national staff requires a shift in focus to the safety and security needs of the latter.
- Armed robbery (of cash, vehicles, office equipment), kidnapping, rape among others may not result in fatalities but are very common threats to aid agency personnel.

2.5 Arguments against organisational changes

Four arguments against prioritising and investing in improvements in safety and security management, appear with a certain frequency in some senior management circles:

- 'We are not in the emergency or the life-saving business.'
- 'We haven't had any deaths in the organisation.'
- 'Risk is an unavoidable part of our work.'
- 'We have been managing risk for decades with existing tools and competences, there is no need for additional or new measures.'

These arguments reveal dangerous assumptions:

- That the level of risk has remained the same over the past three or four decades.
- That the only risk that counts is that to the life of (international?)staff.
- That no deaths in the past is a guarantee for no deaths in future.
- That risk is only high in active conflict zones, and therefore mainly concerns agencies with a life-saving mandate.
- That risk cannot be reduced through individual and organisational measures.

These assumptions go against the available evidence and analysis.

2.6 Where are the change-agents?

In general three types of organisational situations seem to exist:

- Change being driven by mid-level managers.
- Change being driven by top management.
- Strong commitment to safety and security for staff by top and mid-level management.

2.6.1 Change driven by mid-level managers

In some organisations mid-level managers are working to convince senior managers of the importance of strengthening overall safety and security management.The attitudes and arguments they are up against include:

- The dinosaur reflex: 'we can continue as we did in the past'
- The ostrich reflex: head in the sand and hope that the problem will go away.
- The armchair mentality: non-appreciation of the reality because one is too far removed from it.
- The accountant reflex:'How are we going to fund this?', 'Not if it costs a lot'.
- The institutional-interest-first mentality: 'Security is a constraint on operationality; operationality brings visibility and cash-flow; the organisation needs visibility and cash-flow to survive, hence security is against the institutional self-interest.'
- The ignorance or false-knowledge syndrome: top managers don't understand what security management is about, or they may have a very narrow understanding of security in terms of protective procedures and devices, which is only one strategy among others.
- A discriminatory attitude:'International staff are capital assets, national staff are expendables.'

Some of the tactics and arguments they use are:

- Referring to the moral responsibility of the organisation towards its staff.
- Referring to the legal responsibility towards its employees, and the risk of legal liability ('safety and security are not options but requirements').
- Showing ways how security can be funded.
- Taking top managers to the field for closer exposure to danger zones.
- Counting on media exposure and pressure and resulting concern for the image of the organisation.
- Creating some allies on the board of trustees or governing board.
- Using the fact that top management cannot really say 'no, we don't care about the safety and security of our staff', to take them at their word.

2.6.2 Change driven by top management

In other organisations the resistance lies more with mid-level operational staff, in HQ and in the field. Some of the attitudes and arguments they are up against can be very much the same:

- The dinosaur reflex.
- The ostrich reflex.
- The institutional-interest-first mentality.
- The career-interest-first mentality: keep quiet about training needs, management weaknesses and even incidents if they might negatively affect your chances of promotion.
- The adrenaline-addict syndrome: risk-taking gives a thrill.
- The A-type personality: action-oriented, very driven, hard to restrain.
- Solidarity under threat: stay with endangered populations even if you can't do much to protect them.

Some of the tactics and arguments they use are:

- Making public statements of concern for the safety and security of aid agency staff to demonstrate top-level commitment.
- Designating a high-level security focal point to oversee organisational strengthening.
- Creating an *ad-hoc* task force or standing working group to review safety and security practices and initiate changes.

- Drawing up a corporate policy on security.
- Demanding full briefings and reports on serious incidents, and closely following the management of a crisis.

The differences in attitude among senior managers are poignantly expressed in response to internal resource-allocation demands. Where managers are not committed, the attitude is one of 'security expenditure is the first thing we can cut'. Where they are committed: 'expenditure on security is never blocked', and 'using the security argument is the best way of getting a request accepted'.

2.6.3 Commitment to safety and security throughout all levels of management

This is the ideal-type situation. Here committed mid-level staff are actively supported by the executive, to the point that they actually would not want top management constantly involved in the micro-management of incidents and danger situations.

At least three elements characterise the general organisational culture of this latter type of organisation: a culture of care for staff; a commitment to competence and professionalism; and a commitment to being a learning organisation.

The importance of top management commitment was succinctly expressed by one interlocutor: 'Safety and security do not start with the type of staff member you recruit, it starts with the type of chief executive you recruit.' Certainly one organisation, after working in and eventually withdrawing from a high-danger area, made security expertise a key requirement in the next chief executive recruitment.

Generally, boards of Trustees do not play much of a role with respect to the organisational culture on safety and security. An individual board member may take a more active interest, some boards will want to be kept informed about major incidents or crises, or consulted about (general) major investments decisions, including those about security. Some organisations will be more proactive, occasionally briefing the chair on progress in strengthening safety and security. This may reflect a more general way in which executive management works or does not work with its board, rather than a relationship specific to safety and security.

Chapter 3
Management structures

3.1 Management models

Three types of management structure are in vogue:

- The management-line model: The responsibility for security management lies in the operational management line only (centred around the geographical managers at HQ and the HoD in the field), and in that sense is part of the overall management responsibility that includes personnel, finance and programmes. This model can be found in a number of NGOs.

- The specialist security officer model: One or more specialist security officer are located in HQ, and more specialist field security officers (FSO) are deployed in high-risk countries. This is the predominant model in the UN (exceptionally in the UN system, a UNHCR FSO can be tasked also with the security of camps for displaced people - in our terminology we would call this 'protection'). Some NGOs have deployed specialist security officers in high-risk field operations, without necessarily having such specialists at HQ. The authority of specialist security officers is typically subordinate to that of line managers.

- The security adviser model: This combines the above approaches: the responsibility for security is clearly vested in the operational management line, but the security focal point provides specialist back-up. This back-up can encompass taking forward policy articulation and security training, participation in interagency initiatives on security, quality control of field-level security plans, security management audits in the field, specialist support around certain crises, security-related equipment assessment, and the provision of advice upon request from a line manager. This is the predominant model in the Red Cross Movement and is being introduced by some NGOs. This approach is less inclined to deploy specialist field security officers. Security advisers have little or no management authority, but their advice carries weight.

These can be considered ideal-type models. Small permutations are possible. Importantly, agencies over time may also evolve in their approach: one agency for example started out with a management-line approach, and then recruited a full-time security adviser because of the difficulties line managers were having with substantial other responsibilities to take security management forward. Another agency for some years had the security adviser model, but has since strengthened the competence in management line, and let the security adviser post fade out.

3.2 The 'security focal point'

The concept of security focal point (SFP) has found its way into aid agencies but in practice covers a variety of roles and responsibilities.

In agencies with the type-a management-line model, a line manager additionally can be nominated (or in a less formal way simply become, because of his/her personal competence) the (SFP). In this case the person is expected to play a back-stopping role of security adviser, while having substantial other management responsibilities. People in such a position generally indicated the inability to fulfil all these expectations, and there is a need for either more SFPs, or preferably to make it a full-time post. Agencies with tight funding or a high dependency on institutional donor funding, may (be forced to) adopt this approach as it does not require extra staff costs. Agencies with more generous funding but limited exposure to high-risk areas may also adopt this approach, as security may not require the same intensive attention and supervision as others with higher exposure.

BOX 2: Security expert concepts

- A senior manager as security focal point: This can be a senior manager in HQ, typically in the emergency unit, the operations department or HR. The person has other management responsibilities. S/he is chosen as SFP because of his/her knowledge about the subject and because of his/her rank within the organisation. Within the UN system, there can be such focal point on security in the field, on an interagency basis. This person is called the 'designated official' and reports directly to UNSECOORD in New York (see Van Brabant, 2000:annex 3).

- A security adviser: A full-time post in HQ dedicated to security. No formal management authority, but influential because the whole organisation is dedicated to competent security management. The post may co-exist with that of a health and safety officer in HQ.

- Security officers: Full-time staff in HQ and/or in the field, dedicated to security. They are also outside the operational management line, and often subordinate in rank to operational managers. Sometimes logisticians in HQ and/or the field are given security officer responsibilities added to their logistics responsibilities.

In at least one operational UN agency, with a type-b set up with specialist security officers, there is also a SFP in a more senior management layer. The post-holder has other management responsibilities but chairs the internal task force on safety and security. Such an SFP needs to be knowledgeable but not necessarily have the most in-depth expertise. This is a set up to deal with the organisational realities of more hierarchical organisations, where the specialist security officers might be of lower rank than managers.

In type-c models, the security adviser is likely to be the only SFP. The primary role of a security adviser can evolve over time. One such person looking back over several years in that post, identified three major phases: first, the emphasis was on the transfer of expertise with a gradual shift in the balance between the security adviser acquiring knowledge and expertise (learning) and giving expertise to colleagues (teaching); then a phase in which the role had inspector characteristics, while the knowledge and skills were being consolidated in staff competence and throughout the organisation's practices; after that his role had become more one of lighter quality control, occasional back-stopping and monitoring of new threat and response technique developments.

3.3 Locating safety and security expertise in headquarters

The specialist emergency organisations have located their security experts in the Operations Department. Organisations with much 'development' programming, but which also carry out emergency response work, tend to locate the security expertise in the emergencies, disaster response or logistics departments rather than in the wider operations division. This practice should be questioned. At first sight it looks logical because this is the unit that will send staff most frequently to high-risk areas, but the drawback is that it may delay raising awareness and developing competence in the development side of the house and acknowledging safety and security management as a corporate responsibility. Given that a rise in crime accounts for an increasing percentage of incidents, and that the threat of crime may actually be smaller in acute conflict situations, and bigger in so-called developmental settings, it seems important to raise awareness and develop competence also among the non-emergency staff.

It is more of an exception to find the security experts located in the human resources (HR) department, or with management services. Some organisations that previously had their security experts in human resources, have shifted them to operations, where they feel closer to reality. This seems a sensible step. A HR department, however, has important roles to play in the management of safety and security, and bringing or keeping it on board is an important organisational challenge. Two events that were mentioned as having facilitated the mobilisation of HR were the integration of a previously separate international personnel department into the general HR department, and taking senior HR staff to the field to see the conditions of work first hand. Stress counsellors may be found in the operations department and/or in HR. Health and safety advisers are most often found in the HR department - this can be a legacy from past legal requirements to involve employees in the development of health and safety guidelines.

A rather exceptional, but not unique, HQ set-up is that of a 'context unit'. A major characteristic is that its staff is not absorbed by day-to-day demands but is allowed -and expected - to stand back, reflect and analyse. Two possible models seem in vogue:

- A policy and learning emphasis: One or a few people are tasked with monitoring trends in the operating environment and international policy debates and developments, and work on drafting the organisation's position on various issues. This may include taking a lead also on safety and security policies and guidelines. In addition, this unit may be asked to find ways of strengthening the organisational learning ability (more development-oriented organisations would call this a policy unit).
- The strategic situation analysis: One or a few people are tasked with monitoring developments in a country or region, concentrating on the bigger picture and possible scenarios. This can both provide a foundation for advocacy and more contextual policy development, but there is a closer link with operations than in the first model.

3.4 HQ-field relations: authority, responsibility and lines of communication

General organisational good practice demands that authority and responsibility are clearly delineated, so that there is no doubt who is accountable for what.

3.4.1 Authority and responsibility at headquarters

Perhaps surprisingly, in type-a (management line) and type-b (security officers) approaches, formal management authority seems to play a bigger role than in the type-c (security adviser) approach. Where security lies in the management line only, it is important that sufficiently senior management takes responsibility for it, to ensure that security figures actively on the agenda of the most senior management team. Such high-level representation can come from the director of operations. One agency has upgraded its manager of the disasters response team to director level, to enable this. Another expression of the seriousness with which security is treated is that, in case of non-availability of the normal line manager at headquarters,

problems are referred upwards, not downwards to a junior post.

With specialist security officer (type-b) approaches, where security expertise has been developed largely outside the central operational line management structure, and junior in rank to it, a common complaint of the specialist security officers (in the UN but also in NGOs) is that their advice carries little weight and is not infrequently ignored or overridden by line managers. A possible solution, at corporate level, is that the specialist security officers report directly to a very senior official. The problem is a common organisational one: responsibility without authority. The major weakness of this approach is obviously the delay or neglect of putting security more squarely within the line-management responsibilities.

In type-c approaches, the authority and responsibility lie with the line managers. But although without formal management authority security advisers find that their advice carries weight, because senior management and the organisation as a whole accord much importance to security, and because of the demonstrated competence of the postholder(s).

3.4.2 Authority and responsibility in the field

The structure and allocation of expertise in security management at field level is an area that requires attention. There are internal and interagency aspects to this.

Internal aspects: In principle, the HoD as most senior manager has full responsibility for the safety and security of all staff (and assets) in a given operation. In practice, that person has other responsibilities and may not have the time, nor always the interest or the competence. Not infrequently safety and security management or components thereof, are then delegated to the field security officer, the logistics officer, the administrator/office manager and a medical officer. Box 3 identifies some important managerial attention points.

Most if not all of these staff members are based in the country office, typically in the capital city. What appears less clear in current agency practice is the situation with regard to safety and security management in deep-field operational bases at provincial or district level? Beyond ensuring that the staff there has reliable communications, not so much thought seems to have been given yet to how to ensure competence in safety and security management there, and how to organise the management responsibilities. Given that staff in field bases are often closer to the frontline or more exposed to a variety of threats, and therefore need their own locally adapted security planning, this seems an area for urgent attention.

Interagency aspects: Although each agency must retain ultimate responsibility for the safety and security of its own staff, there is need, and scope, for significant interagency collaboration. One obligation would be that of sounding the collective alert. Direct interdependencies can occur when, for example, an agency relies on the medical facilities or the evacuation logistics of another. Indirect interdependencies exist where the choice for one security strategy over another can have repercussions on the collective image of aid agencies, and the relative vulnerability of another one. There is scope for collaboration, for example around context analysis and risk monitoring, centralising security and incident information, establishing a common emergency channel, bringing in technical experts or specialist trainers, and liaising with

BOX 3: Delegating or abdicating responsibility?

- Does the 'delegation' of the responsibility for various aspects of safety and security management lead to an 'abdication of responsibility' by the country manager, or does it constitute a valid team approach, that s/he coordinates into an integrated picture and management approach?
- Where does the administrator get his/her competence from, to understand and manage personnel issues from a safety and security point of view?
- How can it be ensured that a logistician can devote enough time and attention to security issues, especially when there are intense operational demands?
- How to avoid a conflict of interest, or incompatible responsibilities, when a logistician is charged with taking actions to help implement the programme but perhaps is also forced to recommend caution and non-movement in light of security concerns? Some organisations in which logisticians are given an important role in security management, do so under a broad, rather than narrow concept of 'logistician'. These people are effectively deputy representatives. They are also given clear guidance: in case of doubt, security prevails over implementation i.e. err on the side of caution.

Problems can arise, when the security officer in the field advises a particular course of action, which is then ignored or overruled by more senior staff. When this concerns a serious issue, or when there is a breakdown in the working relationship between the HoD and the security officer in the field, there has to be a clear procedure on how to resolve this at a higher level.

Tasks must be delegated, because the HoD cannot attend to everything personally. A team approach also offers the value of 'a second opinion'. But it has to be clear that this is a delegation of tasks, and not of responsibility, in other words, the HoD remains ultimately responsible and accountable.

the authorities (see Van Brabant, 2000: ch. 13-14). More interagency collaboration is often hampered by the sometimes misplaced belief that it amounts to an abdication of responsibility by the agency itself. Although there is now growing recognition of the potential benefits of collaboration, for security competence and capabilities, formal guidance given to field staff tends to overlook it. The HoDs need to set the tone and scope for interagency collaboration, while the implementation of specifics can be delegated to other staff members.

3.4.3 Lines of communication and of reporting

Streamlining the communications and specifying the reporting lines is a general challenge for good management. As the various graphs on pages 18 and 19 show, there is considerable scope for confusion with regard to safety and security management.

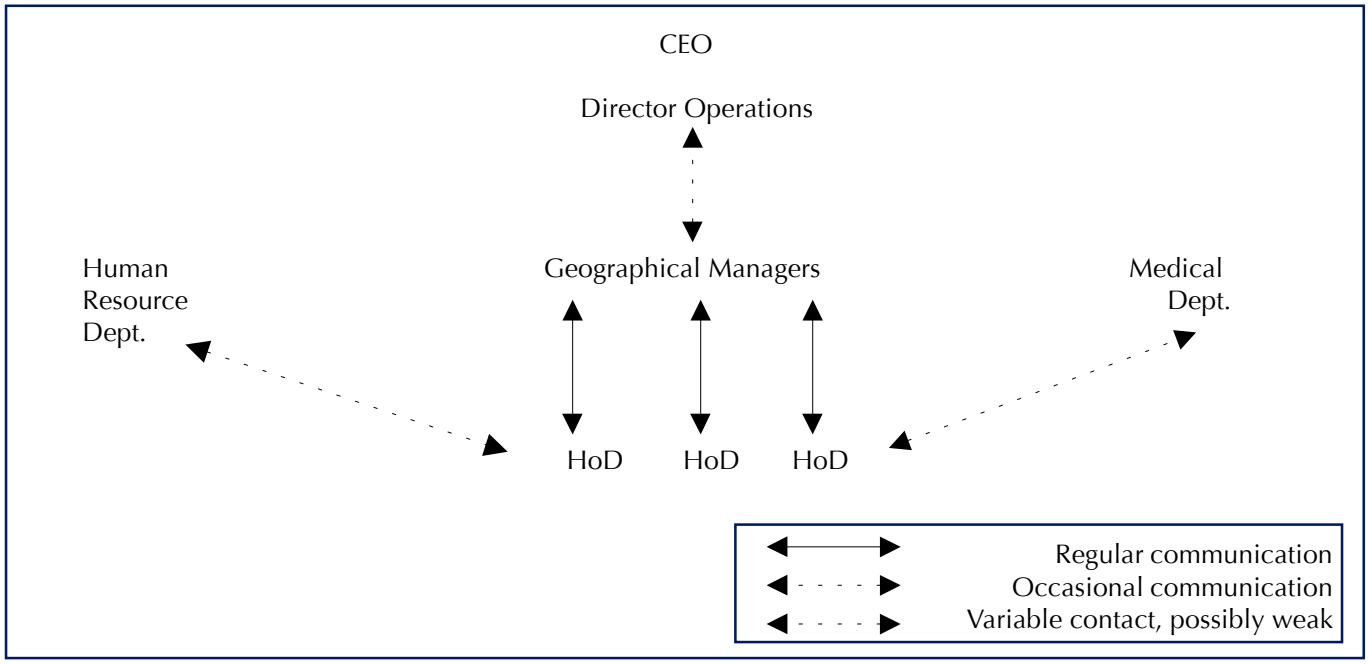
3.4.4 Clarity of decision-making

The above indicates the need for a strong management approach. One organisation, which has consciously decided to retain a strong culture of voluntarism, finds that this seriously delays and complicates decision making, as everybody wants to have a say. This does not seem acceptable when it comes to safety and security.

HQmay restrict that delegation for certain selected scenarios related to security - even in decentralised organisations in which a lot of authority is delegated to the HoD. Common issues on which HQ reserves the decision-making authority are: entering into or returning to a high-risk zone; overriding a decision by the field not to withdraw or evacuate; the overall management of a serious hostage or kidnap situation; the use of armed protection; and, sometimes, the use of a private security

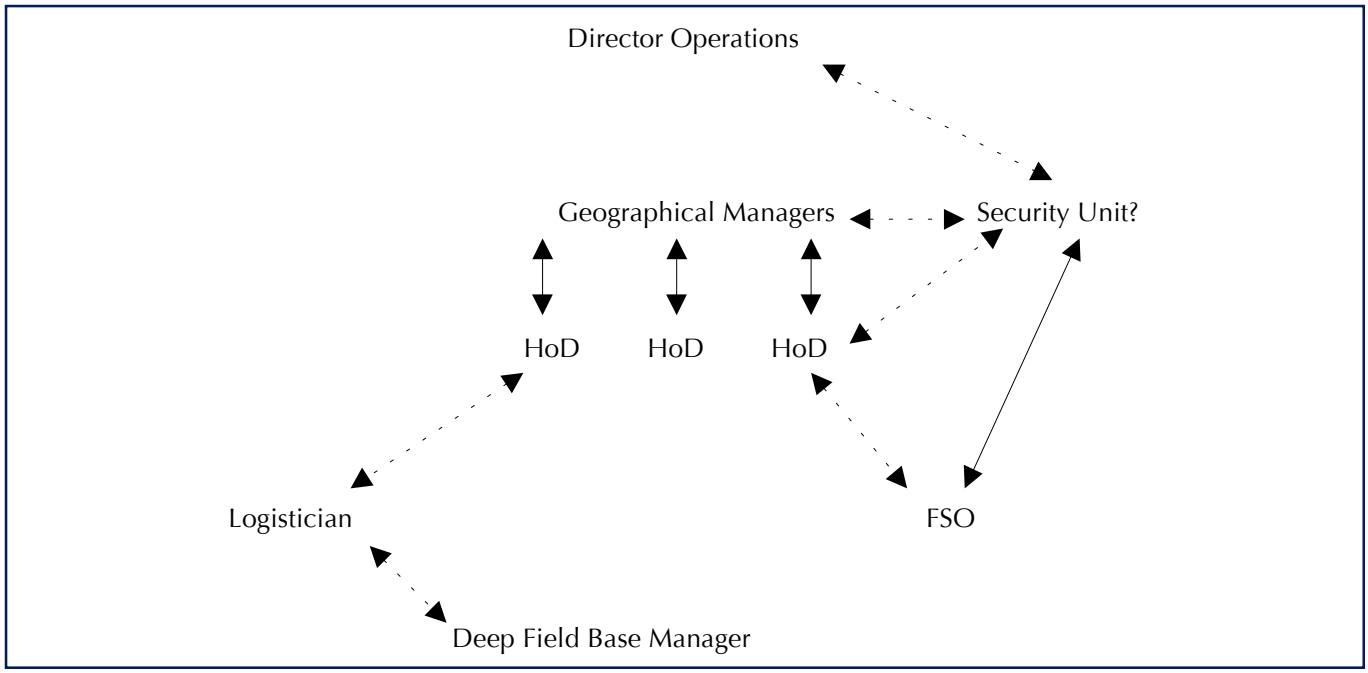
HQ–field relations: authority, responsibility and lines of communication

Figure 1 The management line approach



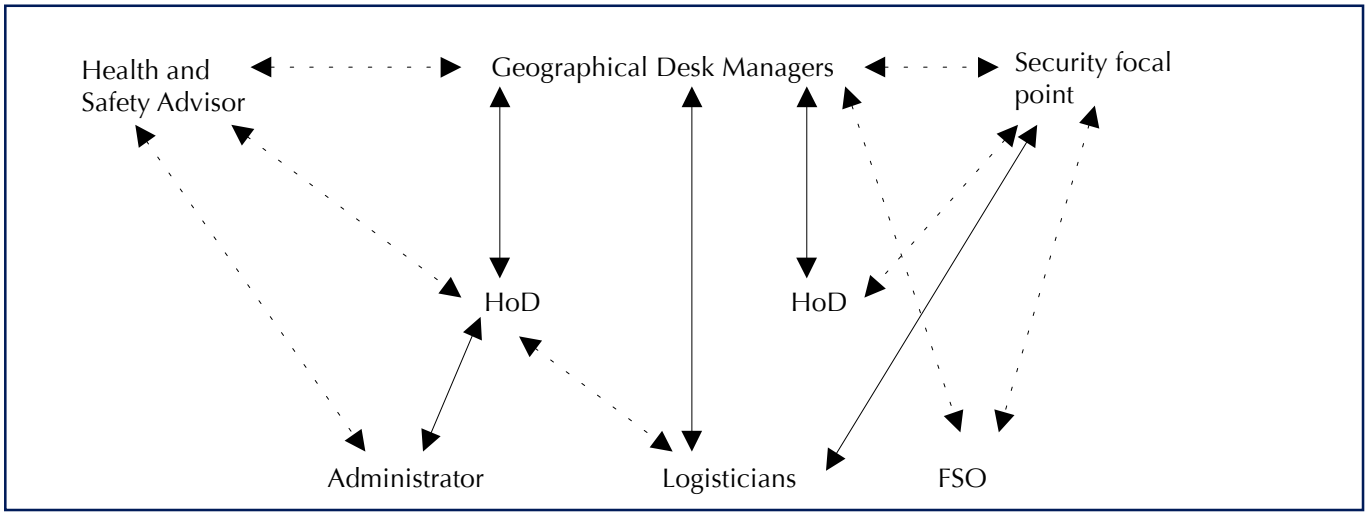
This is the simplest model, with safety and security management fully integrated in the normal management line, either out of necessity (no money for designated posts) or because managers have become competent. The human resources and medical departments will come into play as and when needed, around health and safety issues.

Figure 2 The security unit –field security officer approach



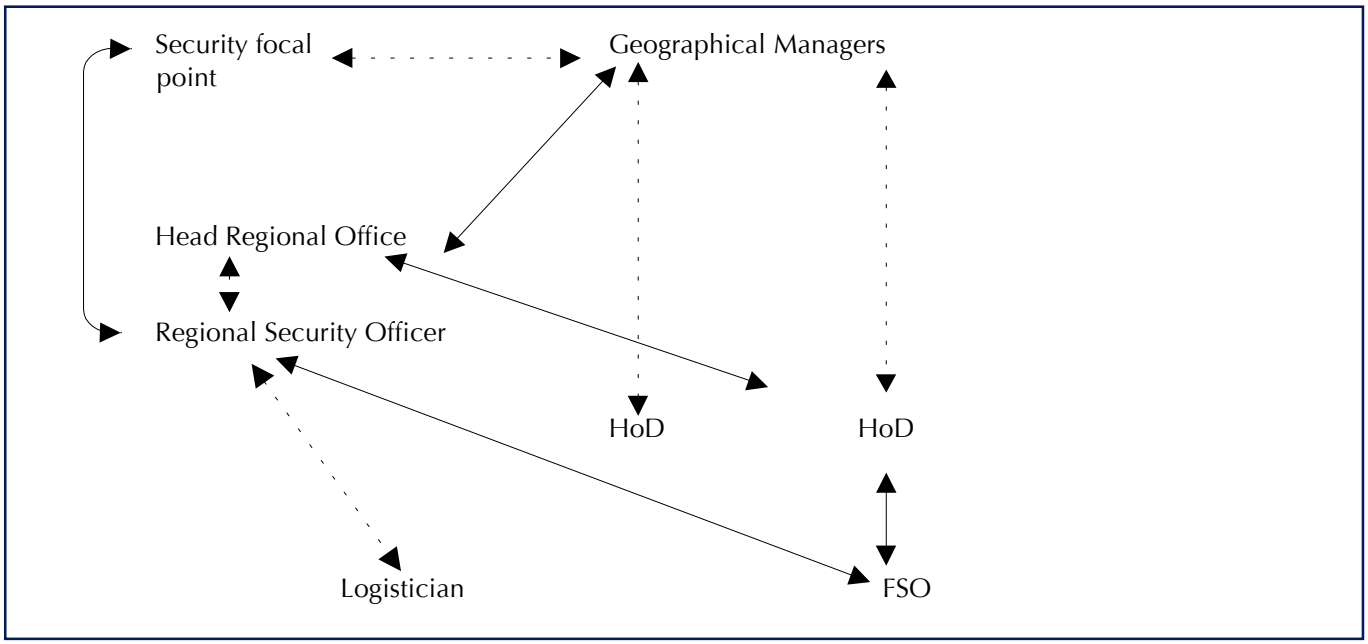
A key question becomes to whom the security officer/security focal point reports. In organisation with flatter management structures, this may be fairly straightforward, for example the director of operations. But in more complex structures, it may be less obvious: does the security focal point report to the emergencies/disaster team manager, or to the general operations director, or perhaps even higher up, to a deputy-director (vice-president) or even the executive director/CEO him or herself?

Figure 3 Diffused responsibilities, confused communications?



The graph shows the amount of confusion that can arise when there is too much delegation of tasks by line managers, to specialists at HQ and to subordinate staff in the field. Communication from different people in the field, assigned safety and security responsibilities, with different posts in HQ need to be streamlined. This requires clarification of what needs to go through the central management line, and what can go directly to focal points? Some organisations work in task forces around operations or have even adopted a formal matrix-management structure, in which case information will flow quickly to all concerned. But that is not always the case, and there can be real barriers between and within departments. Keeping everyone informed should not be an excuse to diffuse responsibility and accountability. It has to remain clear who is responsible for what, and how decisions are taken in case of differences of opinion.

Figure 4 Headquarters –regional office –field relations



The situation becomes more complex when organisations also operate regional offices. Often there a degree of confusion about the managerial authority and responsibilities of the regional office that finds itself between HQ and the country programme. Ambiguity and confusion in issues of safety and especially security need to be avoided at all cost, as likely to have negative consequences. Suppose a scenario in which the HoD normally communicates with the regional office, but the security focal point is at HQ and not in the regional office, is it then clear that as far as security is concerned the communications are directly with HQ? Can security be separated from other programming and management concerns? Should there be a security officer or a security focal point in a regional office? Under what conditions, with what authority and responsibility?

company.

Chapter 4

Management tools

4.1 HQ fora

Where in headquarters does discussion about safety and security take place? Three different mechanisms were identified, which roughly correspond to different stages in the organisational developments around safety and security management:

a. The ad-hoc *working group:* This tends to be created when a problem is identified as serious enough. Its task can be to conduct an internal review of policies and practices and make recommendations, or it can focus on a more narrowly delineated problem such as the drafting of a corporate policy on security, the development of some operational security guidelines, a training plan, or discussing and drafting a code of personal behaviour. In theory an *ad– hoc* task force can be composed of interested staff volunteering to participate, or staff with specific competences or staff with specific responsibilities in various departments of the organisation. Ideally a senior manager is involved, to give the work credibility and to take the outcomes up with the senior leadership. The main problem is what happens when the *ad-hoc* group dissolves - how will momentum be sustained, who will ensure that recommendations and plans are followed up and implemented?

b. The standing working group on safety and security: This mechanism tends to be created when top management is convinced that change is needed, and changes are being introduced. This group usually involves people from different departments in the organisation and has more clout, not only to define and study issues but also to drive various organisational initiatives such as policy development, establishing priorities and resource allocation decisions. It will more actively monitor progress in implementation. Poorly chaired or side-lined by top management as one more committee among many, it can still be ineffective or lose momentum.

c. Safety and security in the operations team and the senior management team: This tends to become the situation when there is a strong safety and security culture throughout the organisation, together with a degree of competence. Safety and security are now mainstreamed. Particularly in directly operational, emergency-oriented organisations, finance, human resources, medical services, communications functions are sometimes closely integrated with operations, and the operations director(ate) becomes a locus for maintaining and strengthening effective safety and security management. Safety and security issues will also come on the agenda of the meetings of the overall leadership (usually bringing together the executive director and heads of all major departments or divisions) as need arises - for example when significant investments or changes are considered, or a serious crisis is being experienced. Under this set-up it is possible again to create an *ad-hoc* working group. But now there is a clear platform that will take over when the *ad-hoc* group dissolves.

4.2 A (safety and) security review

Some organisations have conducted a comprehensive review of policies, procedures and practices regarding security (and safety). Good reviews would include extensive consultation with staff, also with those in the field. A review can be internal, say carried out by an *ad-hoc* group of staff, or it can be conducted by an external consultant. The advantages of external consultants are that they are not caught in the internal politics of the organisation and may be franker and more objective in their analysis. On the other hand, it is also important to understand the nature of the organisation and the constraints it has to operate under.

The outcomes of a review require follow-up action. If top management is not strongly committed, or does not give it sufficient priority, the report may be shelved, or otherwise lose momentum. Therefore a mechanism needs to be in place to develop a management plan for follow-up.

In recent years aid agencies have made significant progress in their understanding of safety and security management and there is broad experience of implementing organisational change. Any such review currently undertaken therefore must be built on the knowledge and experience already been gained in the sector, and not start over from scratch.

4.3 Clarifying the security concept

A first step, as we have seen, is clarifying what is meant by risk management, safety and security, where they overlap and how they differ, and where they don't overlap with the protection of populations in danger. But having done so, another important precondition for making progress is developing a common understanding of what security concept is appropriate for aid agencies. Box 4 identifies three possible concepts.

4.4 Security strategies and security management

Some years ago, this researcher produced a diagram, the so-called 'security triangle', to represent three ideal types

BOX 4: Organisational security concepts

Corporate security: Security here has connotations of site protection, protection of confidential corporate information, VIP protection of executives (for example against kidnapping or blackmail), and protecting the organisation from liability through insurance and legal clauses. It would be wrong to believe that no senior executive or board member of an aid agency could possibly understand security in this way.

A purely defensive security concept: Security here has connotations of protective procedures (no-go areas, curfew times, convoy driving, checking-in of visitors to the premises...) and protective devices (helmets, flak jackets, barbed wire, radios). This is a fairly widespread concept.

A multi-dimensional security concept: Security here brings into play the values and principles of the organisation, its mandate and mission, contextual analysis and scenario monitoring, positioning among and relation to a multitude of actors in a particular context, the nature and design of the field-level programmes and the way it manages all of its staff.

It is this last concept that has been developed under the security management training course and that is captured in the field manual (Van Brabant, 2000). It is now sometimes being referred to as the 'NGO security concept' which is not entirely accurate. Not all NGOs understand security management in this way, and it is certainly also the ICRC concept.

of security strategies: acceptance, protection and deterrence (Van Brabant 1998a: 18). In a nutshell, an acceptance strategy tries to reduce or remove the threats by increasing the acceptance for an aid agency's presence and work in a particular environment. Another way of putting this is 'winning the hearts and minds' of people. A protection strategy does not affect the threats but tries to reduce an aid agency's vulnerability, through protective procedures (no-go zones, curfews, convoy driving) or protective devices (high walls, barbed wire, flak jackets, blastwalls or - where there is respect, - a prominent logo). A deterrence strategy essentially tries to contain a threat by posing a counter-threat (arrest and fines, international sanctions, trial by an international tribunal and, ultimately, armed protection with the possibility of return fire).

Different security strategies require different staff skills and time allocation: a protection strategy requires mostly technical knowledge and is least context specific; an acceptance strategy is most context specific and requires political, social and anthropological understanding, and diplomatic and negotiation skills, as well as significantly more time spent monitoring contextual developments.

This 'security triangle' has been very successful, not so much because what it said was totally new, but because it gave simple concepts and simple words to things that aid agencies had been implicitly practising all over the world. It would be a mistake, however, not to read the commentary with the triangle, and therefore to misuse it. Some agencies seem to have grasped on to 'acceptance' and declared it their security strategy. This could be a dangerous mistake. The commentary says that many individuals, organisations and even countries seem to have a preferred style, but that the art of security management is choosing the right mix of strategies, in accordance with your threat and vulnerability analyses in a given context. To put it simply, an acceptance strategy is not going to prove very effective against brutal organised crime.
The security triangle cannot be taken in isolation, its place and use needs to be seen in the context of a comprehensive security management framework (see Graph 5).

4.5 An organisational safety and security policy

Few of the agencies consulted have a safety and security policy. It is possible to develop a policy relating specifically to security and another one to safety, or to integrate both.

What is a safety and security policy? A key statement acknowledging risk, the responsibility of individual staff members and of the organisation to reduce risk, and the fundamentals of how the organisation intends to do so.

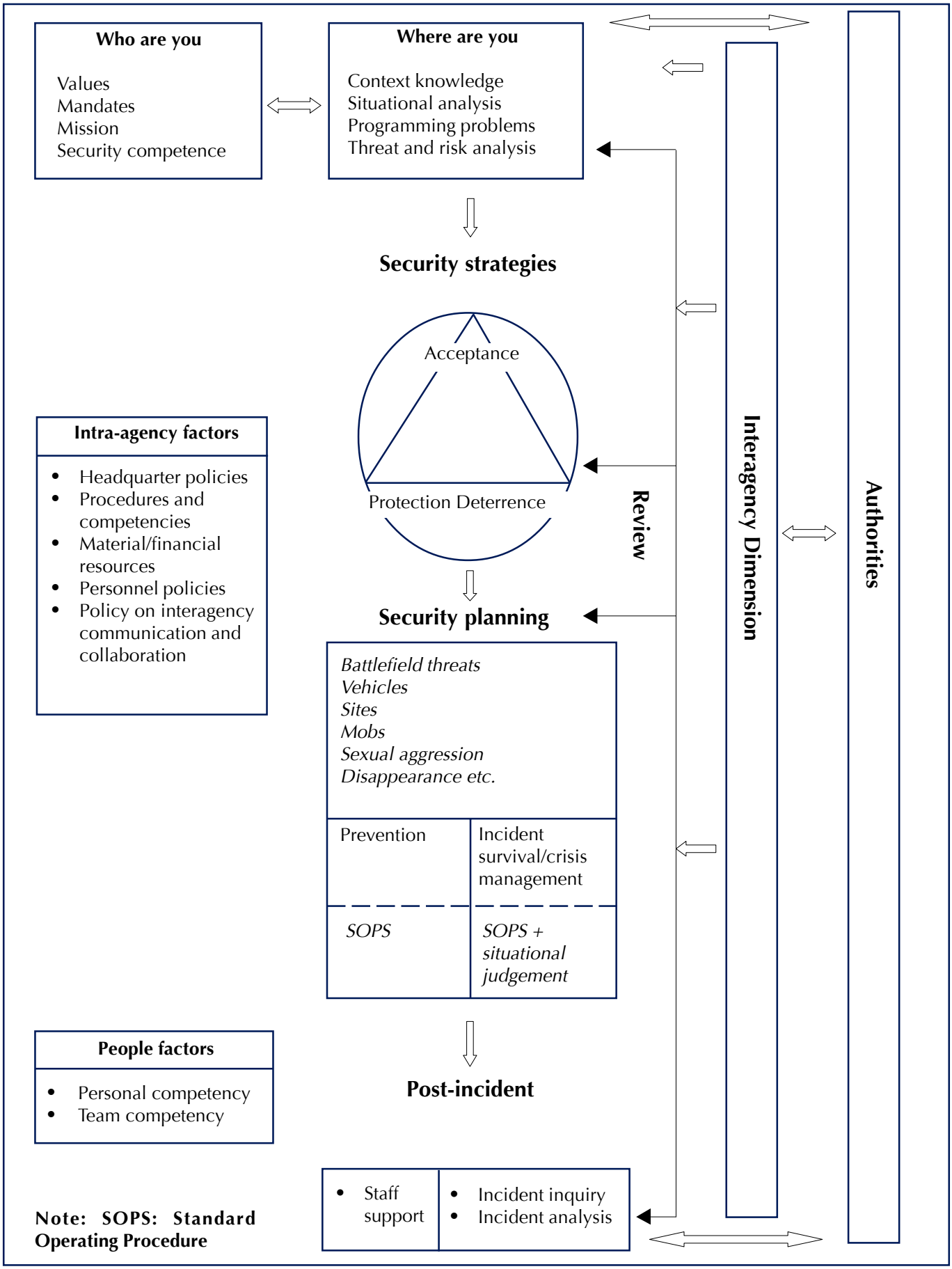
Why a safety and security policy? It is a signal to all stakeholders, staff, trustees, management, partners and donors that the organisation takes the safety and security of its staff serious.

It also obliges management to act, and legitimises the allocation of staff time and other resources to improving safety and security management. It expresses the commitment of the organisation, and thereby becomes a key reference for accountability. In other words, it makes safety and security an organisational and corporate issue rather than an operational one.

When a security policy? It may be premature for an organisation with little knowledge about security issues and how to manage them to try and articulate a policy.

continued on page 28

Figure 5 The Security Management Framework



The reflection of what should go in the policy, and how to phrase it, by itself however will be an important step in developing better understanding. Several organisations have been working on improvements in their security management for quite some time without any policy. The time may now have come to articulate such policy, to more firmly anchor the commitment of the organisation and of top management. A policy can be reviewed and improved.

What should be put in a security policy? Box 5 gives a suggested list of contents. This is largely derived from consulting existing policy documents.
An organigram visualising management responsibilities for security, a copy of the code of personal behaviour, guidelines on security and crisis response planning etc. can be attached in annexes, or incorporated into the additional security documentation for managers.

BOX 5: Suggested content of a security policy

a. General introduction, definitions and basic principles:

- a general statement acknowledging risk in our work;
- a clarification of what is meant by safety and security;
- a general statement that individual staff members and the organisation have a responsibility to try and reduce risk, and that the organisation commits itself to do so;
- basic principles in the organisation's philosophy and practice with regard to security management (the pillars of its safety and security philosophy and practice);
- a statement on the weighing of potentially conflicting objectives, e.g. assisting people in need versus security; witnessing/public advocacy and security; gender policy and security policy; the security of personnel versus that of assets; and
- the status of the document.

b. Basic principles in the relationship to external actors:

- a statement on the basic position of the organisation towards national laws and local culture and customs;
- a statement of basic principles that will inform the organisation's position with regard to the national authorities, armed protection and the use of private security companies, as seen through the lens of safety and security; and
- exception clauses to the previous paragraph on the basic position, indicating who is authorised to agree a departure from it in special cases.

c. Basic principles in the relationship between individual staff and the organisation:

- A statement on the responsibilities and freedoms of individual staff members notably with regard to the right not to go into a danger zone or to withdraw themselves from such without prejudice to their careers; the obligation to adhere to the personal code of behaviour, the obligation to report incidents and to alert other agencies to potential threats; the mandatory nature of security guidelines and disciplinary action in case of breach.
- A statement on the responsibilities and obligations that the organisation accepts with regard to the security of their staff, referring to:
  - a commitment to include a risk assessment in any general assessment;
  - who decides on going into/returning to a danger zone;
  - who decides on withdrawal from a danger zone;
  - a commitment to develop competence in security management/incident survival;
  - the need for security planning and crisis preparedness;
  - the responsibility of management, and the fact that tasks can be delegated but not responsibility;
  - a commitment to incident analysis;
  - a commitment to provide insurance cover;
  - a commitment to manage stress (also cumulative stress);
  - a commitment to provide full medical and psycho-social support;
  - the extent of the organisation's commitment in case of arrest, abduction, sexual assault to the staff member concerned and his/her family;
  - the extent of the organisation's commitment to nationally recruited staff.

As a rule, guidelines should be separated from a policy statement.

One argument in some organisations against developing much written policy is that it creates more bureaucracy and will lead to an undesirable bureaucratic culture. That is a real risk. But there are powerful arguments for putting things on paper: apart from legitimising management decisions ('as a manager you are looking for the support of the organisation, and that has to be explicit') and resource allocations, it also reduces inconsistency in organisational practice. That will increase the confidence and loyalty of staff.

4.6 Financial management and funding

4.6.1 Expenditure lines

Insurance, equipment and infrastructural upgrading, training and staff salaries constitute the major budget lines for safety and security expenditure.

Until recently the most common and biggest expenditures for security probably were for communication equipment and on training (in-house or external). There may have been hesitations and different opinions, especially among donors, about expenditures on larger numbers of guards.

For many organisations, new expenditure requirements are coming into focus. One of these is for increased site protection, owing to a rise in crime and armed robbery. A second one is the need for pre-positioned security equipment (such as telecoms for vehicles and base stations and material for site protection) to be used in initial risk assessments and in the deployment of the first wave of emergency response personnel. With insurance providers, it might be possible to negotiate a reduction in the premium, if the organisation shows that it is investing in risk-reducing measures.

4.6.2 Financial management

In organisations where management is not very aware or not very committed, the belief is 'security is the first thing that can be cut'. In others, where there is strong management awareness and commitment, there is no debate about expenditure when it comes to security.

Communications equipment by and large is already included in the programme and project budgets. But pre-programme financing is required to equip the emergency response teams with the necessary security equipment and competence. The task of such teams is often to carry out more in-depth needs assessments, and to design the projects and programmes, for which institutional donor funding will then be sought. Their security equipment (and safety and security training) cannot await the release of institutional donor funds, it has to be there at day one. That requires up-front funding. One organisation maintains a 'preparedness account' with the agreement of donors. Another is contemplating setting up a revolving fund, which will then be (partially) replenished from programme and project budgets as institutional donor money becomes available.

Training tends to have been budgeted for as a separate activity, for which not infrequently institutional donors have been approached. In the face of staff turnover, the challenge here is to maintain a budget for training and staff development. One organisation has already agreed with virtually all of its donors that an extra 3 per cent would be added to the cost of every expatriate position, to be devoted to training. It then decided to allocate 1per cent of this 3per cent for security, and thus constituted a fund that would continue to be replenished, at least as long as it deploys expatriate staff. It is now seeking ways, however, to devote money to other security-related expenditure.

Only very few organisations have already reached the point where safety and security is fully written into operational budgets as a matter of habit. Several want to move in that direction, but still need to instil the habit in field staff. An argument against budgeting for safety and security as a percentage of total programme costs, is that for various reasons the agency may wish to maintain a presence in a danger zone, but with very limited programme activities. Such percentage allocation then might not suffice to cover the required expenditures. Additionally, some reserve fund probably has to be kept available centrally, to cover unexpected and non-budgeted requirements, for example the sudden need to strengthen site protection in response to a rapid rise in crime.

It is sometimes difficult for agencies to fund headquarter staff positions such as that of a security focal point. This is certainly the case with those that are more heavily dependent on institutional donor funding. , Security focal points based at HQ or in regional offices, whether part or full time, ideally also get an operating budget of their own. This will avoid dispute in the field over who pays for a field visit, and will also allow them to undertake other activities not directly related to operations, such as contacts with other agencies, and providers of security equipment.

4.6.3 Perceptions of institutional donor attitudes

Most agencies feel that donors have become receptive to security and are prepared to fund most expenditure for it, although HQ posts and 'preparedness' accounts may be more controversial. They also recognise that some governmental aid administrations in recent years have actually been in the driving seat to improve safety and security management. Still, consistency in policy or interpretation among portfolio managers in donor administrations has sometimes been a problem; this may require donor aid administrations to develop internal guidelines for their project managers.

Donor attitudes to expatriate field presence should also be looked at from a security point of view. Some donors require expatriate presence for controlling purposes (this is also a basic policy decision of some NGOs). This does

not take into account the relative 'vulnerability' of expatriate and national staff.

There is unease however among some aid agencies about donors using 'security, linked to funding, as leverage for influencing where agencies go and can't go'. Specifically mentioned in this regard are ECHO and the UK government (rightly or wrongly some aid agencies have seen some DFID funding decisions for Sierra Leone and Afghanistan, based on security arguments, as politically motivated).

4.7 Staff stories and memorials

Apart from bringing safety and security into the induction course and offering further training, another way of raising and maintaining staff awareness is to include accounts of staff having experienced risk and incident in the internal newsletter or magazine.

Given that fatal incidents and accidents can play an important catalysing role, it is remarkable that not more organisations honour and remember the staff members they have lost, or who were seriously physically or emotionally affected, for example through memorials. UN organisations seem to have been more attentive to this than NGOs. Memorials can include a plaque or photographs in the building or a memorial service. National staff should not be overlooked. Apart from their symbolic and emotional functions, memorials can also be a management tool to draw attention to and maintain awareness of the fact that aid work is a risky business and that all aid workers have a collective responsibility for their own safety and that of their colleagues.

Chapter 5 Implementation

5.1 Operational Reinforcements

5.1.1 Risk Assessments

Specific risk assessments should take place when entering into a dangerous environment for the first time, or when returning to it after a withdrawal. The overall aim of a risk assessment is to help the agency

- decide whether it will enter into/return to a danger zone;
- to identify the security measures required to be able to do so.

Major objectives of a risk assessment would be to:

- identify the potential threats and vulnerabilities of aid agencies and their staff;
- determine what capacities (competences, resources) would be required to reduce the risk;
- determine what contacts, relationships, positioning and image would be required to generate widespread acceptance for one's presence and work;
- determine the balance between the scale of need and the degree of irreducible risk (the emphasis is not on access *per se* but on potential impact; if the needs are more acute and concern larger numbers of people, an agency might decide to accept a higher degree of risk);
- establish a threshold of acceptable risk from the outset, which will serve as benchmark for future monitoring.

Gradually a change in organisational culture is taking place within agencies, whereby risk assessment takes precedence in timing and importance over other considerations. This is a reversal from the action-oriented attitude, whereby the drive to be in first, to get highest visibility, occupy the most interesting locations and stake out the most interesting programme sectors and operational areas, were major driving forces and incentives for staff, leading to high-risk-taking behaviour.

Giving precedence to risk assessment tends to generate a more gradual, step-by-step approach to geographical and activity expansion, in line with the iterative and cumulative nature of learning about a context and developing relationships. But it also means that programme design gets influenced by the risk assessment: for example, the choice of the amount of stocks kept and the location of warehouses; whether the agency uses its own vehicles or not; whether a high or low visibility strategy will be adopted; and whether special emphasis needs to be put on dissemination and information about its mandate and role in the situation.

In this regard, the question whether to return to the northern Caucasus in the context of the second Chechen war (since mid-1999) has been a major learning exercise for some agencies.

Current management approaches include:

- checking the advice of the home government (for example on the website of the UK or the US foreign offices);
- developing a check-list or a question sheet for risk assessment for the emergency response team;
- sending in a staff member who happens to be particularly knowledgeable about the area concerned;
- sending in the security focal point from HQ to do the assessment.

It does not seem justified to rely uncritically on the risk assessment of a local partner, especially as the organisation's role as employer means they are ultimately responsibility for the safety and security of its own staff.

Most agencies recognise that their competence at risk assessment is still very limited. Some are beginning to mainstream it through developing or including it in the training for their emergency response teams, who would be the first to go in, with full safety and security equipment, for the first few months.

5.1.2 Neutrality and/or impartiality

Several interlocutors saw the pursuit of neutrality in a fragmented and conflictual environment as part of an acceptance and therefore also part of a security strategy. Neutrality may be in their charter or seen as present in the 1994 Code of Conduct of the Red Cross Movement and International NGOs (although the code does not explicitly mention 'neutrality' in its 10 points).

At the same time, in several organisations there is hesitation or internal debate about neutrality either as a matter of principle or whether it can be achieved in practice. In principle, some staff feel that it does not go together well with other values and principles, such as perhaps solidarity and social justice (see Slim and McConnan, 1998: 21). In practice, neutrality may be an intent, but is very much in the eye of the beholder. Neutrality needs to be gained, which requires a very good understanding of the various parties to a conflict and their dynamics. That justifies investment in political and socio-economic analysis. Neutrality also needs to be maintained, it is very fragile: 'security is a tailor-made work that you can rip up in one night'. But even if one's presence and actions are

intended to be neutral, they may inadvertently affect the conflict dynamics and therefore no longer be perceived as neutral. Elsewhere the (security) situation may make it impossible to operate in the territory of all the parties to the conflict. Some therefore feel that impartiality, understood as programming in a non-partisan way, is a more realistic aspiration than neutrality.

The question of neutrality can become prominent for:

- Organisations that also have a political mandate, such as the UN or the OSCE (Serbia under Milosevic, for example, had been suspended from participation in OSCE fora).
- Faith-based organisations operating in environments where other faiths predominate or where a conflict is framed in religious terms (for example, northern Nigeria, the Indonesian Maluccas).
- Organisations with a humanitarian and a witnessing/protection/human rights mandate.
- Organisations working with and through local partners. What if the local partner cannot or does not want to be neutral? Remarkably, several interlocutors mentioned that in such circumstances they had stopped working through local partners. One organisation, because it wanted to work in a certain country, therefore decided to go operational instead.

Agencies invoking neutrality need to clarify, in the first place for their own staff, what they understand by that concept, and especially what it means in practice, namely how does one operationalise neutrality? Does one do it on a case-by-case basis, and is that possible, or does neutrality require consistency across situations and over time? How far this can take an organisation can be illustrated from the facts that MSF did not want to take funding from NATO countries for its work in the Former Republic of Yugoslavia, and that the ICRC has negotiated agreements that it will not be called upon to testify to the International Criminal Tribunal for the Former Yugoslavia or the International Criminal Court so as not to be suspected of using its work as a pretext to collect evidence.

One practical operationalisation of neutrality that an increasing number of aid organisations now recognise, is ensuring a good mix in the composition of its national staff, when working in a religiously or ethnically fragmented environment. This has an impact on how one is perceived, but more actively can also yield a wider network of relationships which are important in an acceptance strategy. Note however that this may not fit with a certain interpretation of an equal opportunities employment policy, in the sense that professional qualifications are not the only criterion for recruitment.

5.1.3 The security plan and planning for security

The security plan has historically been the pillar of the security management of many aid agencies. In practice, its production mainly fulfilled an administrative requirement and the plan remained a dead document with little effective reduction of risk (Van Brabant, 1997).

The current situation across aid agencies sees different approaches to security planning. In several agencies the following types of approach correspond to a gradual evolution as the understanding of effective security management deepened.

Type 1 practice: There are no security plans or protocols. The security protocol essentially consists of advising staff not to go into danger areas and not to go around after dark. Staff may also be given security booklets from other agencies.

Type 2 practice: Country offices have security plans, but they are of unequal quality and inconsistent in content. Common weaknesses are that the plan is produced by one individual, is not based on a broader context analysis and a more specific threat assessment, only gives standard operating procedures and tends to be primarily built around security-alert phases and evacuation guidelines. Safety measures may have been partially or completely overlooked. In some cases, the security plan from one or a few country offices are circulated within the agency; several country plans may then simply get copied from others with little more than a change in date, and in the names of the author and the location. The document is given to all staff, who are made to sign for it, a formalistic gesture to reduce liability in case of accident or incident. There is little further active reference to the plan.

Agencies who have no operational presence but work exclusively through partners, may have guidelines for field visits, which may suffer from similar weaknesses as the above type of security plans.

Type 3 practice: Having identified the problems with type 2 practices, the agency now develops guidelines for security planning, which put emphasis on the process of developing a plan, the team character of the exercise, and provides the major headings or topics that need to be addressed. A generic template is developed, which needs to be adapted locally. Field teams may still have difficulty finding out exactly how to generate the information.

Type 4 practice: The agency sees the security plan no longer as a plan but only as one tool among others in managing security. Maintaining alertness, active monitoring of the environment, proactive scenario thinking, analysing incidents, strengthening of awareness, competence and discipline are other important tools. The safety- and security-related documentation now constitutes more than one item. The overall security management becomes more refined with more emphasis

put on overall context analysis and specific threat assessment; vulnerability analysis is refined with differentiation in the vulnerabilities of different operational bases (each base now has its own plan rather than all relying on a country-wide security plan) and different staff (females, different types of national staff); and the preparedness goes beyond standard operating procedures to try and avoid an incident, to include guidance on incident survival and on immediate incident or crisis response (with again possibly differentiated responses such as for the withdrawal of national staff versus that of international staff).

5.1.4 Quality control

Several agencies have adopted practices intended to bring an element of quality control into the safety and security preparedness.

One of the most common ones is for each field office to send copy of its plan or other security documents to HQ, for review. A template, or a broader question and attention point sheet, then provides one benchmark for HQ. A related common practice is for desk managers or emergency officers in HQ, to prompt the field office regularly to review their security preparedness. But without in-depth knowledge of the local context, it is hard to know whether the security measures put in place are comprehensive enough and appropriate.

Opportunities for a more in-depth review of the risk analysis and the appropriateness and completeness of the security measures adopted, may be provided by a field visit from the security focal point or from an operations manager from HQ with a wider range of objectives. A field-based internal or interagency training course on security management can be another opportunity. This may or may not lead to a report in writing.

More formal would be the security review or audit, whereby a staff member from HQ or one or more consultants visit with the explicit purpose of reviewing the overall risk assessment, the security measures in place, and the discipline and competence with which they are implemented. Such a security review can be prompted by concerns in HQ, but can also be requested by the field as a supportive action. The wider organisational culture, and the attitudes and relationships of managers, will influence whether it is more of a policing action or more of a management support exercise. Such a security review has to be reported on in writing.

Mentioned by only one organisation consulted were evaluations in which weaknesses in the security management were highlighted. Explicitly writing safety and security management in the terms of reference of programme evaluations might begin to yield important insights in the dynamics between security and programming.

5.1.5 Incident reporting and incident analysis

a. Incident reporting

Incidents need to be reported to HQ for:

- operational reasons: it helps HQ staff to monitor the context, and may provide them with perhaps important information when it comes to crisis management;
- management reasons: it allows the development of internal statistics, which will become one indicator to monitor the effectiveness of improvements in security management. The individual agency statistics can then also be shared with other agencies for a wider trend-analysis (Van Brabant, 2000: annex 1; Sheik et al., 2000).

A few of the agencies consulted felt confident that HQ knew about almost all incidents. Most agencies felt that HQ was likely to hear about serious incidents, but by no means all. Some agencies reported this to be a very weak area, with many incidents never reported to HQ. Agencies specialised in emergency responses, where desk officers maintain almost daily contact with field managers do tend to be better informed. The presence of a field security officer also tends to improve the reporting of incidents. On the whole this is an area in need of management attention.

Clear guidance needs to be given to field managers but also to all field-based staff on what characterises an 'incident' that needs to be reported. Specific guidance is also required that incidents that affect other agencies must be reported, as well as narrowly avoided incidents (still an indicator of threat). At the same time, attention should be paid to the fact that incident reports may have to be adapted for circumstances where confidentiality about the victim or details of events, even within the organisation, is a major consideration. This applies certainly to cases of abduction and sexual assault (see Van Brabant, 2000: chapters 12,13,16).

Only one agency mentioned that it had clarified to its staff what it understood to be a reportable incident. It seems logical to set different parameters for what should be a reportable incident for field staff to the HoD, and for what the HoD should report to HQ.

There are obstacles to incident reporting, that work at the level of individuals:

- Danger habituation: Field staff have been so often exposed to threats and risks that they consider most things happening not worth mentioning; a 'macho' attitude can further contribute to this, but it can affect everybody;
- Frequency of incidents: There are so many incidents taking place all the time, that it becomes impossible to report all of them. Reporting here will take more the nature of pattern and trend speculation, and scenario-thinking (see Van Brabant, 2000: ch.4)
- Unconfirmed rumours: There is talk and rumour about incidents but no useful confirmation of what

took place or even that it did take place. This can also apply to incidents that allegedly affected another agency, which it does not want to talk about.

But particularly problematic is the existence, in some organisations, of disincentives against reporting incidents to headquarters. Box 6 summarises some common facilitating and inhibiting factors.

At least two projects have paid attention to incident reporting: People in Aid and the Humanitarian Security and Protection Network (HSPN), run under the auspices of VOICE (Brussels). PIA offered a course 'Setting the record straight', drawing on incident report forms that are commonly used by organisations in our home countries. The HSPN developed an incident reporting and preliminary incident analysis form, that can be installed on a laptop, and allows the production of a fairly comprehensive report in a very short period of time. After the first two years the project had made very little impact, even among the NGOs piloting it. This appears partially due to initial project design flaws, one of which was its isolation from a larger security-management approach. The tool, however, does have merit and there is no intrinsic reason why it should not be considered in the context of a larger management approach.

b. Incident analysis

A few agencies will fairly systematically analyse why an incident or crisis came to occur and how it was managed. Even these have not yet institutionalised the practice. For most organisations, however, this is an even weaker area than incident reporting. The sharing of incident analyses occurs less and is even more sensitive than the sharing of incident reports.

Some common obstacles to incident analysis are fears that it will reveal individual failures; reveal organisational failures with therefore potential implications for legal liability; or touch on delicate political sensitivities, within or outside the organisation.

This reflects an organisational culture which sees 'critical review' and 'evaluation' as fault-finding and punitive, rather than as learning opportunities and a component of increased accountability. The critical review of incidents and crises and how they were managed, should trigger a review of the whole security management in place in a particular context, and offers valuable learning more generally (see Van Brabant, 2000: ch. 16).

Ways of improving and institutionalising incident analysis are:

- Including it in the overall security policy, thereby making it mandatory.
- Inscribing it in the terms of reference of an HQ forum, with sufficiently senior management involvement, that supervises the analysis taking place and asks challenging questions.
- Occasionally commissioning an independent enquiry and analysis.
- Ensuring that the analysis is documented and that, like incident reports, the analysis reports are centralised.
- Ensuring that the analyses are referred to and drawn upon as part of the learning cycle (case material in training), and for further improvements in overall organisational security management.

BOX 6: Organisational factors inhibiting and facilitating incident reporting

The most common inhibiting factors are:

- Programme protection: The belief that HQ will interfere with ongoing programme operations when hearing about an incident.
- Career protection: The belief that a report of an incident will be taken as a failure of the field manager, and thereby may negatively affect his or her career prospects.

Factors that encourage the reporting of incidents to HQ are:

- Explicit mention in individual and management responsibilities, and supervisory attention to it.
- Insistence by top management that every serious incident is reported to them.
- Inclusion in pre-departure orientation and in-country arrival orientation.
- Clarification of what constitutes a serious incident.
- Inclusion of a subheading on incidents, under a level-1 heading on security, in the template for situation reports.
- Provision of an incident report format.

c. Incident report sharing

Incident reports need to be shared with other agencies on the ground, to alert them to the existence of a threat, to obtain security-related information from other agencies, in a give-and-take manner and to build up a database for incident mapping and incident pattern analysis, one technique used in risk analysis (see Van Brabant, 2000: ch. 4). There is a confusion about the sharing of an incident report when it comes to sexual aggression of a staff member. Protecting the confidentiality of the victim remains a prime concern, but when a sexual assault has been committed by an actor external to the organisation, other agencies need to be alerted to the threat (see Van Brabant, 2000: ch. 12).

With regard to practices in the field, some agencies express clear commitment to sharing information and provide guidance to field managers to this effect. But overall the reality is one in which information is shared on an informal

basis with those you know and whom you can trust, with levels of trust not generally high. Again, the presence of field security officers, or people with that additional responsibility, may facilitate the information sharing, as they are more likely to get to know each other through regular meetings. Few organisations, formally or informally, actively encourage field managers to share as much as possible, a situation that could be improved. Several organisations do share incident-related information with others at HQ level, but also here the practice appears to be informal and on an *ad-hoc* basis, and limited to those they know and trust.

5.1.6 Armed protection

Many aid agencies at some point have used armed protection, such as bodyguards, for the protection of sites or convoys and vehicle movements. There is some debate about whether in high-risk areas a field security officer should be allowed to carry a (concealed) firearm. Yet few have a policy that goes beyond the statement that staff cannot carry guns, and that arms are not allowed in the agency compounds, vehicles or in hospitals.

Some organisations have a clear policy guideline that holds that they do not want armed protection, but exceptions can be made on a case-by-case basis needing authorisation by HQ. Some of the criteria then invoked are:

- A risk-impact calculation: how many people are in how acute a need of our assistance and would armed protection allow us to (continue to) reach them?
- The type of threat ('yes' to protect from crime and banditry; 'no' to protect from acts of war or politically motivated threats).
- The type of deployment ('yes' for compound protection; 'no' for convoys).

A structured list of questions of principle, of context and of management, that can help managers think through decisions on armed protection can be found in Van Brabant (2000: ch. 5).

5.1.7 Telecommunications and other technical knowledge

For years telecoms (radios/satphones) equipment has been the main focus of security technology. It should be remembered that telecoms *per se do* not guarantee a reduction in risk. It may do so because it allows a rapid spread of the alert, and therefore works preventively. It may not help avoid an incident, but it can bring a rescue team more quickly to the site, and therefore possibly reduce impact. But telecoms equipment itself can also become the objective of attackers, by turning you into a target.

Telecommunications are changing rapidly. The concept of telecoms is evolving, and getting more closely integrated with IT, inasmuch as agencies now want not only voice communication but also (confidential) data transmission, even from deep-field bases or mobile stations. Internal connectivity and confidentiality then become criteria, in addition to reliability and autonomy. The telecoms/IT concept is developing into that of an area-wide network, with increasing interagency compatibility and integration. The move, if individual agencies and donors coordinate to make that possible, is towards a humanitarian telecoms/IT network.

Some agencies, especially those likely to get involved in large distributions requiring convoys of trucks, are also beginning to install vehicle tracking systems.

But there are also non-communications-related technical knowledge and skill requirements that are coming to the foreground. Agencies working in battlefield zones, of which there are many apart from the ICRC, may need the technical skill to construct blastwalls and bomb shelters properly. With the rise in crime and violence in many countries, site protection (reinforced doors and barred windows, safe rooms in residences, extra outdoor lighting, burglar alarms or panic buttons) is becoming a rising concern. It may require additional technical knowledge and perhaps training for logisticians. Some agencies have deployed construction experts to high-crime areas, to reinforce site protection.

Many experienced logisticians and some security officers do not have the full technical knowledge on weapons threats and protective devices against them. This would include precise knowledge on what armour, a flak jacket or a ballistic blanket do and don't protect against. Recently, unexploded ordnance, in particular cluster bombs and depleted uranium, have come to the attention of aid agency security officers. Technical knowledge about them is now being explored.

As mentioned before, organisations with an emergency response mandate, need to have security equipment pre-positioned for immediate use in the very first assessment mission, and have their emergency response personnel trained in its installation and proper use.

5.1.8 Crisis preparedness

Some organisations have thought through their crisis preparedness, while several others are working on it. Others still have given little thought yet to who would or should participate in a security-related crisis management team at headquarters or how to manage different types of crisis. The concern over kidnapping and hostage taking of recent years has provided a major impetus in this, but attention should be paid to overall crisis management unrelated to the specifics of a kidnap or hostage situation.

Good practice in crisis preparedness includes:

- A clear definition of what constitutes a crisis: This can be one affecting an individual staff member, or the

entire operation in a country. The key criterion is whether there has been or may be a serious threat to the physical integrity of staff. This can include death threats, armed robbery, an assassination (attempt), serious injury, loss of life or limb in an accident or in a mine explosion, rape, the bombing of agency premises, and a general deterioration of the security situation forcing hibernation or withdrawal. Financial fraud would not constitute a crisis. A crisis is also likely to be an event that will require the management of communications, internally and with others outside the organisation, and a review of the security measures and the decision to operate in a certain location.

- Permanent contact with headquarters: several agencies maintain around-the-clock contact number, with a system of rotating duty officers. Management considerations around duty officers are: permanent communications (mobile phones), enough staff to maintain a sustainable rotation, full hand-over briefings between duty officers, staff with confidence and sufficient management authority to take decisions; parameters for the level of decision-making authority of duty officers under different circumstances (urgency, higher-level manager reachable or not). In an agency with several security focal points at HQ, these may constitute the duty officers. Others will rotate the responsibility among operational-line managers (desk officers).

- Crisis management teams: Typically these have two or three levels. An incident management team will be constituted at field level and at headquarters. For serious and more prolonged crises however, a strategic direction team can be constituted at HQ level (and sometimes on an interagency basis in the field). The purpose of a strategic management team, is to create a level removed from the immediacy of the management, with the time to analyse, reflect and consider the pros and cons of different response options.

Who makes up a crisis management team: In smaller and less emergency-oriented organisations, this is likely to include a desk officer, the head of the disaster response team, the head of personnel, perhaps but not necessarily the chief executive. Several larger organisations, especially those specialised in emergency response, in HQ already work in a matrix-management structure (on a cross-disciplinary task force basis) around country operations. In that case the incident management team is likely to be the normal task force, but now reinforced with additional staff capacity and additional competences (for example stress counselling, legal advice) if needed, to deal with additional requirements. Depending on the seriousness of the situation, one person may head the team as strategic director (the overall operations director), or a strategic management group is constituted. At least one large organisation is considering setting up an operation or crisis room at HQ, which will have permanent communication and a duty officer, but also provides an adapted physical layout for a crisis management team.

BOX 7: Competence in a security-crisis management team

Three different attitudes or approaches can be identified:

- rely on general experience only;
- rely on general experience with additional guidelines;
- strengthen general experience with crisis management training.

Some organisations, especially those specialised in emergency work, hold that their staff deal with near-crisis situations virtually on a daily basis, and that therefore their experience guarantees competence.

Others have (also) developed supporting guidelines. Among the range of such documents are:

- the protocol for mobilising a crisis-management team;
- general crisis management guidelines, relating for example to the management of communications with internal and external actors, the logging of contacts, communications and decisions, levels and processes of decision-making authority;
- specific crisis- management protocols, for example a kidnap or withdrawal/evacuation management protocol;
- guidelines for the repatriation of a deceased staff member (which requires formal permission from governments and procedures for the airline).

At least one highly experienced emergency organisation continues to organise training and simulation exercises for potential participants in a crisis-management team.

Specialist competences may be brought in from outside for specific crises such as kidnap situations, or arrest and incarceration by the national authorities. Outside expertise needs to be identified in advance.

There are additional points related to crisis preparedness:

- Crisis-management capacity needs to be maintained all the time, even when key people are elsewhere for work or on holiday; this may require the pro-active identification of stand-ins.
- Prolonged crises (several days to several months) may require the capacity to deploy several fully competent crisis-management teams on shifts.
- Crisis-management competence needs to be maintained in the face of staff turnover.
- Developing and maintaining crisis-management capacity is probably easier in specialised emergency organisations than in developmental ones, or multi-

mandate ones with a smaller disaster response unit.
- How a crisis was managed also needs to be formally reviewed afterwards, and the learning therefrom documented and fed back into future competence and practice.

5.2 The management of some specific threats

5.2.1 Abduction and hostage taking

The spate of kidnappings in the Caucasus, especially since 1997, has been very influential in focusing agency attention on this threat. But aid agencies have had to confront abductions elsewhere, in Somalia, Colombia and Sierra Leone. The hostage taking of peacekeepers, such as during the war in Bosnia-Herzegovina and more recently in Sierra Leone, has made it an urgent matter also for the UN Department of Peacekeeping Operations and presumably several national defence ministries.

This type of threat is drawing serious management attention in several agencies, because it can be of long duration, puts at risk the life of the captive, concerns demands for a large ransom with the danger of creating dangerous precedent by paying up, and more often than not draws in the family/ies of the victim(s), the home government, the national government and the media. It tends to be a high-profile crisis in which HQ has an important role to play.

The actions undertaken by some agencies by and large consist of:

- A public policy that no ransom will be paid.
- The inclusion of hostage survival guidelines in security documentation.
- Greater care in the selection of staff for deployment in high-risk areas.
- More detailed briefing of staff to be deployed in such areas.
- Compilation of more personal affairs information of staff being deployed in high-risk areas.
- Reducing the exposure of potential targets (especially international staff).
- Protective measures to harden the target including armed guards.
- The development of a kidnap management protocol within the organisation.
- The identification of external expertise to lead or advise on hostage negotiations.
- The training of security officers in hostage negotiation.

Room for improvement exists in:

- Better distinction between types of disappearances.
- Articulation of a clearer policy of what the victim and family and friends can expect as practical commitments from the organisation. Being briefed about this beforehand can be an important psychological help in incident survival.
- Training through scenario simulations given to the various HQ staff that will become part of the crisis-management team.
- Clarification of key principles of action to deal with national staff disappearances (see Van Brabant, 2000: ch. 13).

5.2.2 Sexual assault and rape

By contrast, sexual assault and rape have so far received far less attention, although there must be at least as many, if not more, such incidents, as there are cases of abduction/hostage taking. The fact that men can also be at risk is even less recognised than the risk for women, and this researcher has not yet come across any documentation among aid agencies about whether the management of a male victim differs from that of a female victim, and if so, how. Most of the agencies consulted indicated that they had made little progress if any on how to deal with this risk.

There is significant confusion about the management of the threat and the incident. Attitudes in agencies vary between:

- It is still almost a taboo, we have only just begun to talk about it and create awareness.
- It is not a taboo, but we don't necessarily want to become alarmist by profiling it.
- It is not a taboo, but can you do anything about it/we don't know what to do about it.
- We offer traumatic stress counselling, just as for any other traumatic experience.
- We want to do something about it, but it is contentious within the organisation as it seems to conflict with our gender policy.
- We acknowledge it, are doing something about it, and staff security here takes priority over the gender policy.

This reflection derives from an interpretation of the organisational gender policy that emphasises the importance of female staff on teams, to facilitate programmes reaching women, and bring greater gender sensitivity to the styles of working. Another possible interpretation, however, would acknowledge differentiated risks for male and female staff, in the same way that men and women also have different needs. In practice of course, both lines of thought are appropriate, and the management faces a dilemma in weighing these different concerns against each other.

Where the risk of sexual assault is beginning to be taken up, frequently this is done from another angle:

- In the context of a sexual harassment and abuse of power policy: this is appropriate inasmuch as it recognises that sexual assault can be committed by another employee of the organisation, but it fails to address squarely cases where the assault is committed by outsiders.

- In the context of critical incident debriefing and trauma counselling: this may be necessary but is insufficient as the response to a sexual assault not only involves attention to the psychological support for the victim, but also has medical, confidentiality of information and potentially legal dimensions. Moreover, Western individual talk-therapy approaches of counselling may be inappropriate for national staff.

At policy level at least three issues need to be addressed:

- In the type of situations in which aid agencies deploy, sexual assault by outsiders can constitute a high risk. There may be a higher risk of gang rape/aggravated assault. This will affect the victim, but also his/her partner, and potentially other staff present who were forcibly prevented from protecting their colleague. This cannot be addressed by a policy on sexual harassment alone.
- Does security override the gender policy? Not deploying or withdrawing female staff from high-risk zones is seen as undermining the operational objective of some organisations to reach more women among the target group or the employment policy of a better gender balance. Female staff themselves may very well resist different treatment for security reasons. The issue however needs to be looked at from a worst-case scenario point of view: is being gang raped, and possibly contracting AIDS as a result, worth the affirmation of gender equality at a particular time and place? One way of overcoming the apparent policy conflict is to base contextual decisions on a pro-active assessment of the threats to and vulnerabilities of different categories of staff (see Van Brabant, 2000: ch. 4, 20).
- The need to protect the confidentiality of the victim has to be balanced with the need to alert others that a threat exists.

Current organisational practices mostly consist of:

- including sexual assault in security orientations and security awareness courses;
- including guidelines for the security of women in the security documentation;
- a selective (for deployments in retroactively identified risk areas) inclusion in pre-departure briefings of female staff;
- the pre-positioning of a cocktail of medicines at field locations, to be taken as soon as possible after the incident, to reduce the risk of contracting a sexually transmitted disease including AIDS (the Post-exposure Preventive Treatment starter kit);
- not deploying/withdrawing female staff from high-risk areas.

None of the organisations consulted appeared to have any documentation in this regard. The 'Rape Response Handbook' referred to in annex 3 on documentation was obtained from another aid organisation, not included in the consultations for this research (but see Van Brabant, 2000: ch. 12).

BOX 8: Managing the risk of sexual aggression

The following are steps suggested to improve the management of this particular risk:

- Face up to the reality of the risk.
- Review insurance policies for their coverage of medical and psychological support costs.
- Develop policy and management guidelines that deal with sexual assault in its own right, rather than under another heading, and principles of communication that recognise the need for confidentiality with the need to alert others.
- Clarify the relationship between the gender and the security policy.
- Articulate the concrete organisational commitments of support to the victim and others affected, for psychological but also medical, legal and financial support, and informing staff of these commitments.
- Explicitly include sexual assault in the initial and ongoing risk assessments in the field.
- Most importantly, develop immediate rape response guidelines for field-level managers and train them.
- Develop guidelines on how to raise the issue with national staff, who may have very different expectations about what they want the organisation to do and not do.
- Enquire from centres working with rape victims on responding to the sexual assault of males.

5.2.3 Sexually transmitted diseases

The aid community is sexually active. High-stress and high-danger situations may increase the level of sexual activity. People also tend to adopt more risk-taking behaviour. Unprotected sex puts one at risk of various sexually transmitted diseases, including, but not only, HIV/AIDS.

Safe sex is explicitly addressed by several of the agencies consulted. It will be included, for example, in the pre-departure health and safety briefing, and in safety and security awareness courses. The tendency is to focus on the risk of HIV/AIDS rather than other sexually transmitted diseases. One organisation offers its international staff the possibility to have a blood sample taken, externally, prior to departure, to be kept frozen, as a reference to determine the period in which infection might have occurred. Several organisations offer returning international staff the option of a test for sexually transmitted diseases, again externally and confidentially.

Several organisations ensure that condoms are always available to national and international staff in the field, and can be obtained discreetly. For some religious organisations, this proves impossible. They limit themselves to advising staff to use condoms.

Not specifically inquired into, is the question whether and how much organisations invest in awareness raising among national staff, especially among potentially higher-risk groups such as drivers and relocated staff.

5.2.4 Safe driving, fire hazards, first aid and context specific risks

These areas were not explored in depth and the following comments are therefore only impressionistic.

Safe driving:

- Several organisations familiarise international staff with 4x4 vehicles on difficult terrain prior to deployment. The inclusion of emergency repair training is probably more rare.
- Other organisations have a policy that international staff cannot drive an agency vehicle. This policy has to be set against that of a local rest-and-relaxation policy. If international staff on longer-term contracts either cannot obtain another vehicle, or have to take along a staff driver when going away for a weekend, the safe driving policy may inadvertently contribute to increased stress.
- No information was provided about driver-trainers for national staff drivers, and it is not clear whether this is a widespread practice or not.

Fire hazards:

- This tends to be a relatively neglected risk. Some organisations are training staff (logisticians, security officers) to conduct safety assessments of buildings with regard to entry and exit points, electrical wiring and so forth, and how to conduct fire drills. A residence/compound safety and security survey form could be developed, which would obviously also pay attention to smoke alarms and fire extinguishers.

First aid:

- First-aid courses are widely available in many countries of operation. It is not clear how good the practice is to provide first-aid or trauma kits (including sterile needles) in vehicles and residences, and whether staff have the desired level of competence. Ideally, the necessary competence levels (who needs to be trained, on what priority basis, and to what level of competence) are determined in light of operating circumstances (for example, in what circumstances does a driver need to know how to provide first aid to a mine victim or someone with bullet wounds?). Some doubt can be expressed that this is currently being done adequately, even within medical agencies.

Another subject that needs to be addressed is to what degree staff should be briefed and prepared for very specific contextual risks such as risk reduction, orientation techniques and survival strategies for working in jungle areas, desert areas (northwest Sudan, the Afar region of Eritrea/Ethiopia) or mountain areas with heavy winter snow (the Caucasus, the Hindu Kush) or when having to use unsafe local boats (Indonesia).

5.3 Improving personnel management

5.3.1 War risks and malicious act insurance

On several occasions aid agencies discovered, too late, that their existing insurance did not cover war risk or malicious acts, or that exclusion clauses applied. More attention is now being paid to the issue. Several respondents indicated that their organisation provided war-risk insurance but very few knew details.

Some valuable references on the issue are Davidson and Neal (1998) and Van Brabant (2000: annex 6) where many points are spelled out. Some additional points are added here:

- Insurance cover is typically dealt with by the human resources department, which can usefully liaise with operations about the real-life circumstances on the ground and what insurance cover therefore would be required. One agency is recruiting a full-time person for four months to review its insurance cover. Legal expertise is necessary.
- A multi-agency approach to insurance companies does not necessarily seem to lead to a better deal than a single-agency one.
- It may be possible to negotiate a lower premium if the agency can demonstrate that it invests in increased competence in safety and security management.
- Attention needs to be paid to whether staff on different contractual status are equally covered. HQ staff, researchers, consultants or evaluators going on short-term missions to danger zones, may require special insurance.
- The question of insurance for national staff is a difficult one. Since 1998, nationally recruited staff of UNHCR is also covered by its malicious acts insurance. National legislation may apply. Mechanisms to create a staff-insurance fund, on a voluntary participation basis, can be explored.
- Insurance cover calculated on the basis of multiples of a victim's annual salary may turn out too low for seriously injured international staff that are paid only a volunteer salary.
- Detailed attention to exclusion clauses is required. Coverage may no longer apply when it turns out that security guidelines were not respected. Insurance companies may exclude certain countries, the list of which may change, so that the agency needs to remain continuously updated. An exclusion clause may concern situations in which the home government is involved in military action; it needs to be clarified how the insurance company understands involvement in a peacekeeping mission. One European insurer was said to refuse to insure US citizens, as they are more likely to turn to litigation.
- One agency mentioned its readiness to provide the financial support out of its own reserves if needed, on the grounds that care for its staff is a core value and that being perceived as failing to do so, would have a very negative impact on its supporters.

5.3.2 Safety and security in the assignments cycle

The term 'assignment(s) cycle' is used here to encompass various stages in the process from recruitment to post-assignment debriefing/follow-up. An assignment(s) cycle does not necessarily correspond to the period of contract. The duration of a contract can be longer and cover assignments to different field postings. Individual agency practices (and capacities) differ, but across agencies the following major phases in the assignment(s) cycle can be identified: recruitment, induction/orientation, pre-deployment briefing (and training), post-assignment debriefing and re-deployment.

a. Recruitment

Across the range of agencies, it is possible to identify different degrees to which security particularly is taken into account at the time of recruitment (shortlisting/ interviewing and testing).

The poorest practice would be one in which the agency looks at the level of past overseas experience in general, and where the only agency initiative would be to get a recruit into contact with the desk officer or the country representative only if and when s/he enquires about security. Many agencies have become far more proactive.

The most common practice among those consulted now is to inquire actively into various aspects relevant to safety and security, in the course of an interview, for example, mental health and general well-being, maturity, cultural sensitivity, coping with stress, social and team skills, fears or concerns about working in a risk environment. This can go together with, or be reinforced by tests some of which are psychological and some of which to get an indication about whether the candidate shows common sense with regard to security or would perform well in a team in a hostile environment.

Several points come up in this context:

- How important is safety and security competence in the recruitment of people to go on a roster; people to go to the field without management responsibilities; people to go to the field with general management responsibilities; desk officers/regional directors based in HQ or a regional delegation as chief executives? For at least one agency, such competence is a key qualification for CEO recruitment.
- How important is safety and security competence in recruiting for specific field posts? Some agencies will assess candidates not just for a general preparedness and ability to work in risk environments, but also how they would function in the specific contexts to which they could be posted, and the competence of the team already in place. Less-experienced and less-competent recruits would not be posted to high-risk zones unless there was a very strong and competent team on the spot. The particular posting then may reflect how the relative strengths and weaknesses of a candidate are weighed against each other. One agency goes even further and looks for more detailed competences in security management, according to context: in some cases security management mayl require especially technical and procedural security competence; while other contexts might require analysis, diplomatic and negotiation skills.
- Organisational culture plays a role here: candidates may be reluctant to express their concerns and fears, as it may jeopardise their overall chances to work with the agency.

That would suggest that something of the organisational values and culture need to be communicated during the recruitment process, so that frank exchanges can take place.

This has several management implications:

- The interviewers/recruiters need to be competent on safety and security to be able to assess candidates.
- Where staff is recruited locally or through regional offices, the same competences need to be present, and similar criteria used.
- More advanced questioning and testing makes for a longer process - agency practices range from anywhere between two hours to two to three days of engagement with candidates. This has cost implications especially in terms of staff time. Bad recruitment has cost implications, financial and in staff time, but these do not show up so well in the accounts, or are largely overlooked in financial management analysis and audits.
- Increased emphasis on safety and security competencies may make it more difficult to recruit as it may rule out certain candidates that score well in other areas. As sector-wide competence in safety and security management improves, this may become less of a constraint.

The intention of highlighting safety and security competence early on in the recruitment process is to ensure that candidates can make an informed decision and that staff deployed in risk zones are competent. The practice however may have an adverse impact on equal opportunities, especially on affirmative policies to promote more women and other nationalities into senior positions. This may require agency- or sector-wide initiatives to equip more women and other nationalities with the required knowledge and skills.

b. Induction/orientation

The larger agencies, with more staff and more resources, tend to organise a general induction/orientation for all staff new to the agency, or at least for staff with management responsibilities. The durations differ, but three to five days is not uncommon.

BOX 9: Bringing safety and security into the recruitment process

- Write competence in safety and security into generic job descriptions, which then allows it to become a point during recruitment, as well as in appraisal and promotion considerations.
- Review and adapt generic job descriptions together with the qualifications deemed necessary and desirable, in the light of the requirements of the particular post.
- Bring safety and security on to a core list of desirable attributes on the recruitment form; possibly test a candidate with some scenarios and case examples.
- Involve the security focal point at HQ in the recruitment for postings in high-risk areas (especially where competence in safety and security is not yet mainstreamed among operational desk managers and personnel officers).

Safety and security are addressed in the induction course, during a session usually ranging from two hours to half a day. It seems useful to review what the aims might be:

- An important area to address will be principles, policies and procedures: the health and safety policy and practices; the security policy, the security concept and strategies of the organisation; balancing safety and security with other objectives and concerns; individual and organisational responsibilities, the mandatory character of certain security rules; the management line for safety and security, personal conduct and incident reporting.
- Another area to address might be basic operational skills: the use of radios, safe driving, first aid, map reading and orientation without compass.
- Some competences should be tested and developed through more simulations, for example defusing anger and hostility, passing a check-point, basic negotiation skills, behavioural discipline with regard to landmines, do's and don'ts under fire. This becomes more time and resource intensive. One agency tries to send every untrained expatriate on a two-day security awareness and communications course prior to deployment. Another agency runs the induction course as a five-day simulation of life in the field, during which candidates are actively exposed to various aspects of safety and security. Here the orientation course in fact is part of the recruitment process: both the candidate and the employer confirm the contract only after this extended 'simulation/exposure'.

Here again there are practical management challenges and opportunities:

- People are not all recruited at the same time, and such inductions cannot be organised for too few staff. But a policy could be that all new managerial staff need to have gone through an induction course within three months of starting their work. However, if the analysis of a recent study, that 30 per cent of the sample of aid worker deaths had died in the first three months of assignment is correct, this time frame may be dangerously late (see Sheik et al., 2000).
- Travel between a field posting and the course location needs to be budgeted for, and field managers need to schedule in the absence of staff during the orientation course.
- Agencies with limited resources or skills in-house may limit their own in-house induction to agency-specific matters and ask an external resource person or agency to organise and run the general safety and security orientation and training.
- Involving staff recruited for HQ postings in the safety and security orientation will help mainstreaming the safety and security awareness.
- People recruited locally or through a regional office can be sent overseas for the orientation course, but some agencies are now also organising orientation courses in the field, which allows them to reach more national staff.

c. The deployment briefing

A deployment briefing probably takes place both at HQ, pre-departure, and upon arrival in country. The term is used here in the narrow sense of a mission or context-specific briefing, as distinct from a more general agency and awareness- or skill-oriented induction/orientation. Mission-specific briefing is becoming more common.

Practical management steps and attention points are:

- Make proactive briefings mandatory. At least one agency requires written confirmation from the recruit that briefings have taken place, as a check.
- Define the key topics that need to be addressed in a mission-specific briefing. One agency has turned this into a check-list. Among them can be: context analysis; the culture and local laws; history of the agency's involvement and presentation of the positioning of the agency in the context dynamics; programmes, projects and partners (also looked at from a conflict and security point of view); specific threats and risks; the context-specific security guidelines and rules to reduce risk and for the immediate incident or crisis response .
- Define what in principle should be addressed by HQ or the regional office and what in the field, but also monitor that one or the other takes over if circumstances make it impossible for either HQ or the regional office or the field to do their planned part.
- People should be frankly briefed prior to departure about specific security threats such as rape, hostage taking, armed robbery, the measures put in place to reduce the risk, and the extent of the organisation's commitment if things go wrong Several organisations do so already. Some organisations also allow staff ready

to be deployed the option to say 'no' and withdraw from the assignment that late.
- Are there context-specific safety threats for which focused briefing or training is required, for example operating in jungle, winter snow or desert conditions, operations requiring the use of ships with poor safety standards?
- Provide appropriate context briefing also to HQ or regional office staff or consultants going out on a shorter field visit;
- Who is responsible for, and included in the briefing? In some organisations, the security focal point in headquarters will get involved in all pre-departure briefings, but more often only in the briefing of those being deployed in recognised risk areas; where security management is mainstreamed in the operational management line, the operational desk managers take primary responsibility also for the safety and security briefings.
- Extend deployment or assignment-specific briefing to national staff. This may require other language skills and significant staff time, and therefore probably a stronger role for a national staff member in the field.
- Formally introduce safety and security in all handover briefings between post-holders. For those charged with management responsibilities around safety and security, that would include the nature and location of records, the risk assessment, comments on contacts and information sources, external support facilities, incidents that need continued follow-up, staff directly or indirectly affected by an incident that need to be watched or receive further attention. .

d. The post-deployment debriefing

Agency practices on debriefing differ. Some do not debrief at all, others only *ad hoc*, others again will debrief only people returning from difficult postings, while some will systematically debrief all returning expatriate personnel. Nobody mentioned debriefing of national staff at the end of their contract.

In the general debriefing (as different from a critical incident debriefing which normally takes place soon after the incident, rather than at the end of an assignment) several agencies actively ask about stress, some about the person's experience of the risk and risk management. Where the staff member or the debriefer identify a need, a referral can be made to an external specialist for more in-depth debriefing and support. Some agencies leave a post-assignment visit to a counsellor voluntary. Others make it mandatory to prevent people stigmatising themselves by opting for counselling. Several agencies have a mandatory medical check-up, again by an outside entity to guarantee confidentiality, but testing for sexually transmitted diseases is voluntary. A few organisations require that the supervisor of a staff member sends an evaluation report, which is then discussed during the debriefing. This can include references to the person's performance in risk situations.

Managerial attention points are:

- Who does the debriefing, particularly in regard to safety, security and stress and does the debriefer have the competence to ask the right questions and note non-verbal signs?
- Can a format with attention points for debriefing be of help?
- How is the feedback gained from debriefings translated into organisational learning and improvement?

e. Redeployment

There is growing awareness, not yet fully translated into practice, of cumulative stress and the need to take this into account in redeployment. Some of the more advanced practices to respond to this are: making it easy for staff to ask for leave-without-pay during deployments; ordering burned-out staff to take mandatory leave; rotating staff between high-risk and lower-risk and accompanied and non-accompanied postings. There are obvious practical constraints here: some organisations have too few posts in more stable, lower-risk conditions, while the need for more experienced people in difficult contexts does not correlates well with the possible equation of more experience equals more accumulated stress.

Some of the more finely tuned attention points mentioned under recruitment, can also come into play with regard to redeployment, notably the question whether the quantity of a person's experience matches the very specific skills and qualities required for a given post (context requirements and team competences in place).

5.3.3 Corporate and individual responsibility

In general it appears that agencies have made progress in more clearly defining the responsibilities of individual staff members, but may still have to define more clearly the organisational responsibilities.

a. Organisational responsibility

Aid organisations are beginning to acknowledge more formally their general responsibility for the safety and security of their staff in a safety and security policy statement. This may signal a change to a greater culture of care for staff.

Yet more attention from top management seems to be required to the precise legal obligations that the organisation incurs as an employer. Some important points are:

- Such legislation is developing and probably becoming more stringent.
- There may be lack of clarity about the legal responsibility of the employer towards staff deployed overseas.
- Clarity is required setting out the legal responsibilities applying topeople on different types of contract (for example, short-term contracts, consultants, subcontractors whose work for the organisation takes them into danger zones).

- National legislation for national staff must be enquired into. This task is probably for administrators or office managers in the field.
- National legislation may prohibit anyone not so authorised from providing medical services - how does this affect the agency's ability to provide emergency care?
- Is the practice of making staff sign a waiver of responsibility at the time of employment, stating that they will not make any claims against the organisation in case of accident or incident, legal by itself, and would it stand up in court?

So far few agencies have experienced court cases from (international) staff or their relatives over safety and security issues, but many respondents felt that the trend is going in that direction. This suggests that a health and safety officer, particularly if such postholder has primarily a medical training, might not be best qualified to monitor legal developments. Legal expertise will be required. One agency was bringing in such expertise for four months, to review the whole issue. There seems significant scope here for hiring expertise on an interagency basis, in the field and at HQ, at least for agencies with their HQs in the same country, and therefore under the same national legislation. Spelling out organisational responsibilities and commitments, however, particularly for specific threats such as chronic disease, sexual aggression, kidnapping, should not only be done for legal reasons. It also enhances the trust of staff in the organisation, may be an important support for incident survival and an indicator of a spirit of care, respect and accountability to those managers like to call 'our most valuable resource'.

b. Individual responsibility

Several agencies now make it explicit that staff in a danger zone may ask to be withdrawn if they feel insecure or are unable to cope. They also allow staff at any point during the recruitment and deployment process to say 'stop', if they have strong reservations about being deployed in a danger zone.

In principle, this individual liberty does not affect the prospects of the employee in the organisation. Particularly crisis-oriented organisations will, however, indicate limits to such individual liberty. These limits arise from three constraints:

- there is always a degree of non-compressible risk;
- they may have very few postings with little risk;
- they may not want to create two categories of staff, one that is always taking the risks and another one that is always in the relatively 'safe' postings.

Therefore someone who wants to avoid most risk may be better off with another organisation.

5.3.4 Personal behaviour

Greater emphasis is being impressed on staff about the fact that security rules are mandatory and breaching them can give rise to disciplinary actions, including obligatory repatriation (or dismissal for national staff). At the same time, codes of personal behaviour also make it clear that staff members represent the organisation 24 hours a day and seven days a week, and must behave responsibly at all times.

Incident analyses reveal that personal behaviour can directly (through drunken driving) or indirectly (through involvement with a local person, cultural disrespect, arrogance) contribute to incidents. Until recently, what staff members did outside their work and working hours was seen as belonging to the private sphere and therefore outside the organisational remit. That is changing rapidly. In some cases it remains at the level of verbal communication, in others the organisation"s position is formalised in the form of a 'Personal code of conduct', 'Code of sexual conduct', 'Lifestyle code', 'The responsibilities of the volunteer' or similar reference.

The arguments are that risk-taking behaviour can endanger the individual and colleagues, but more importantly, that the behaviour of all staff influences the image and perception of the organisation. By articulating a code of personal behaviour, organisations do not necessarily judge the behaviour of individuals, but make it clear that certain behaviour may be contrary to the organisation's values and expectations, and that it therefore is better than both part ways.

Articulating a code is not enough, managers need to be given guidance on how to work with it before, during and after an assignment. Practices include:

- Talk hard but deal gently with problems, except when there are clear security implications which require robust action.
- Include personal behaviour in the assessment of an individual at the end of the assignment by the direct supervisor (that assessment will be discussed with the individual during debriefing).
- Offer support to individuals with a behavioural problem.

A discussion point for management is the scope and formulation of such a personal code. What is phrased in general terms and what is spelled out very specifically? General references to the need for staff to behave with respect and in ways that do not tarnish the image and credibility of the organisation leave room for interpretation. Specific prohibitions will be linked to swifter disciplinary action. Defining precisely what is not admissible will require careful reflection:

- No drug use (there is a legal referent to what constitutes 'drugs', although there are differences between Western countries).
- No alcohol abuse (more difficult to define what constitutes 'abuse'; temperance movements will consider

alcohol a drug, even if its legally admitted).
- Codes of sexual conduct include rules against bringing prostitutes on to the agency premises, visiting brothels, relationships with local people (there may be serious intent), sexual promiscuity also between international staff (when does one become 'promiscuous'?).
- Arrogant and unwarranted authoritarian behaviour.
- Acts of cultural disrespect.

An even more difficult issue is the application of certain expectations also to nationally recruited staff. Drinking and driving is easy, but national staff may argue that in their culture the norms about what constitutes drug and substance use, sexual conduct, and status and hierarchy, are very different from those in Western societies. Behaviour not in line with Western expectations may not necessarily negatively affect the perception of the organisation in the eyes of the larger population. There are sufficient instances of resentment, anger and even violence resulting also from national staff behaviour not to take the cultural argument at face value, but there is an element of balancing of organisational (Western) values and expectations against different cultural and social norms. An approach can be to involve national staff in the discussions and let them come up with what they would define as cause for concern and as outrightly unacceptable, in their social context(s).

5.3.5 Stress

Organisations have become much more aware of stress and the need to manage it. Both internal and interagency surveys have confirmed that staff experience of it is a major problem (for example, Jensen, 1999; McNair, 1995; Salama, 1999; UNHCR, 1997; WHO, 1998).

However, in the responses so far the emphasis has been more on post-traumatic or critical incident stress, to the comparative neglect of cumulative stress and 'burn-out'. Critical incident-related stress is more dramatic and visible. Yet cumulative stress is equally important because it has impact on overall performance, may result in more risk-taking behaviour, affect team functioning, and leads to suboptimal behaviour in security situations. It may also contribute to the break-up of relationships and marriages and is probably an important factor in staff turnover and shorter careers in the field. There is also very limited awareness of, let alone attention to, significant cultural differences in the experience of what Westerners call 'stress' (as a cultural construct), in how people cope with it, and what sort of treatment they may prefer. In certain Asian countries, for example, the first individual response might be fasting to purify the person, and later visiting a monk. Individualised approaches emphasising talk-therapy are not appropriate for everybody.

Box 10 lists a variety of mechanisms that organisations are using to increase the awareness of stress and attention to it.

It must be mentioned that staff in stressful environments are not necessarily very receptive to stress-control attempts.

BOX 10: Addressing stress

- Guidelines on stress and stress management for (all) managers
- Stress explicitly addressed in the orientation/ induction course.
- Stress addressed in the deployment briefing.
- Improvements in field-level accommodation, to ensure more comfort and privacy.
- The development of rest-and-relaxation policies in the field, sometimes made mandatory.
- The use of the 'buddy system' in the field, including the manager.
- Training field managers in basic defusion techniques.
- Awareness-raising sessions on stress for desk managers as monitors of the HoD.
- Cumulative stress as attention point in post-assignment debriefing.
- Cumulative stress as attention point in re-deployment decisions.
- Rotation of staff between high-stress and low-stress postings.

Two obstacles are the 'cowboy-mentality' ('we can take everything'; 'you shouldn't be in this job if you can't take it') but also the A-type committed personality, with a high sense of solidarity who does not want to rest while so much work still needs to be done. What causes an individual stress, and how much, is partially a personal matter, and monitoring is made difficult by the absence of clear benchmarks. But it is possible to identify some of them (perhaps together with the individual staff member).

Several organisations have been seeking ways to mobilise more competence on stress management, although, as mentioned before, the emphasis has sometimes been more on traumatic stress. Mechanisms in use are:
- A professional consultant on a part-time basis. This sort of external resource person may be tasked with running awareness sessions, providing training, developing a policy on stress, providing advice and guidance to the field by telephone, and, in critical cases, go out to the field.
- A roster of external mental health professionals that can be called upon for deployment to the field after a critical incident.
- In-house training of a number of counsellors, based in headquarters or in a regional office, who can be mobilised to do critical incident debriefing (more skilled emotional first aid) both for a repatriated person, as well as for the whole team in the field (not only those directly involved in an incident or crisis suffer from critical incident stress). Mostly these staff members have other primary tasks, but they can be deployed when need arises; the scope of their competence and responsibility would remain problem identification and debriefing, treatment and extended counselling would

be done by outside professionals that staff are referred to. It is important to remember here that these people know the limits of their competence and are careful not to overstep it; at least one organisation has reached the point where it is now consciously selecting people for training in this role to get a better gender and language balance. Another organisation mentioned that staff could get external treatment on a cost-sharing basis - the question is whether this would be covered by the insurance, and to what degree.
- Training of peer-support volunteers among field staff. The initiative for this training comes from the staff themselves and is not dependent on the field manager. Their tasks are to monitor overall stress levels, do first-line stress defusing, report to HQ or the regional delegation on the types of problems they encounter (rather than identifying individuals in need), and identify locally available expertise and resources.

Field-security officers do not often seem to get tasked with stress management, although some are trained in first-line defusing techniques.

A more difficult and relatively less examined question is that of monitoring the stress levels of the HoD. Some security focal points, based at HQ, would pay attention to this during field visits, but perhaps more promising is the raising of awareness and training for operational desk managers, who are the line of contact for the HoD in the field. Attention is also required to the stress levels of those who themselves are actively involved in crisis management.

One organisation mentioned the additional potential social support role of its network of returned volunteers, for staff just returning from assignments.

5.3.6 Categories of staff

a. International staff

Attention is to be paid to the safety and security management requirements of international staff with different contractual status:

- There may be different insurance clauses depending on the type and length of contract.
- Short-term consultants or evaluators going on field visits.
- People based in the field for longer periods, but on a consultant contract.

Is there a same sense of moral and legal responsibility, and similar insurance cover, and are they being provided with competence and support for their safety and security management?

b. National staff

The most problematic area however is that of nationally recruited staff, the level of support they get, and the limits of responsibility that an organisation accepts for their safety and security.

The question of local staff safety and security remains a painful weakness in the aid sector. There remains strong resistance even to face the issue:

- 'because of their work with an international organisation, they are already privileged among local people, should we privilege them even more?';
- 'risk is their own responsibility';
- 'this is totally context dependent, and tremendously complex, what can we do?'.

The reflection on national staff security is often reduced to the question of evacuation across an international border. Often this is not something that international aid organisations can organise or guarantee. This has led some simply to add a clause to national staff contracts that the agency will not be able to evacuate them. Some arrangements may then be made to provide some financial support to help national staff reduce the risk or find a safe place. The obsession with the evacuation question can make agencies overlook the facts that national staff are vulnerable to stress, health and safety threats, and to being victimised by other acts of war or violence such as landmines, armed robbery, ambush, hostage taking and rape. It also hides the fact that Western responses to problems such as stress, rape or kidnapping may not be socially or culturally appropriate, never mind helpful, when it concerns national staff.

Some mid-level managers try to argue for more agency initiative because national staff:

- Are an equal moral, if not legal, responsibility of the organisation.
- Are a cornerstone of programme implementation.
- Often protect expatriates from their own inexperience.
- Often play an active and sometimes crucial role in security management.

Moreover, the global trend is for fewer expatriates and more national staff. Some agencies are even beginning to think of developing regional and national rosters of potential recruits to draw upon.

Even where there is awareness in HQ, the responsibility to develop safety and security measures for national staff may be entirely left to the head of delegation, without much further guidance or support. More proactive and committed practices are still very new and tentative. Box 11 overleaf lists some of them.

5.4 Competence: knowledge and skill development

5.4.1 External resources

Aid agencies make use of external resources in a variety of ways: to provide legal advice, insurance, medical evacuation/repatriation services and mental health

BOX 11: Addressing national staff safety and security

- Discipline: can national staff discipline be imposed in the same way as for internationals, can their movements be restricted in their own living environment as they might be for expatriates, or can they be subjected to a similar code of personal behaviour as for Western expatriates?
- Training: some organisations are now actively involving national staff in orientation/induction courses, in security awareness and security management courses, particularly through moving training more to the field or the region; a few are also training nationals as trainers.
- Responsibilities for security management: if expatriate administrators, logisticians, or deep-field-based programme managers can be given security-management tasks and delegated responsibilities, can and will these also be given to nationals in such positions? Can national staff be designated as security officers, where this does not pose a major risk to them?
- Specific vulnerabilities: a more explicit and more sophisticated analysis of different vulnerabilities within the group of staff — men or women, expatriate or national staff, different subcategories of national staff — is still a fairly new practice.
- Policy guidance on benefits: some organisations already extend full insurance cover also to national staff, either through an international or national insurance, or through self-insuring by the agency. Others are working on a medical and social insurance policy for them, perhaps costing different scenarios. Those that make condoms available to their staff, will also ensure that they can be confidentially obtained by national staff.
- Policy guidance on organisational responsibilities: some organisations have already taken the clear decision that national staff are entitled to their full support, when they are threatened or affected because of the nature of their work or because of the fact that they work with an international agency. Others have articulated some general guidance principles — that national staff and international staff should be exposed to the same levels of risk (which may differ according to the context), and that the agency accepts the responsibility to take national staff home or to a safe place elsewhere if home would not be safe.

counselling or post-traumatic stress treatment. They also use them for example to review organisational policies and practices in general or in a specific operational setting, to develop training materials for internal use, to provide training and to provide advice on basic principles in the management of certain crises. Several aid agencies give published manuals and resource materials on safety and security, developed by others (NGO, Red Cross and UN) to their staff. Others draw on existing material to develop their own manuals.

5.4.2 Safety and security documents

Annex 3 provides a rough overview of the variety of documents that can be found in aid agencies. While their existence is an indicator that agencies take safety and security seriously, there are also serious weaknesses that require management attention. There is a great quantity of reference documents mostly for field personnel, some for HQ personnel. Within one agency the available documents combined may amount to anything between 15 pages and two full binders. It is worthwhile, however, to think critically in advance, or review, the existing documentation. Box 12 offers a number of critical questions with which to review the existing material.

5.4.3 The competencies of security officers

There is a mainly informal debate about whether security focal points and security officers should have a professional security background, namely be ex-military or ex-police. On the surface of it, this is one of the elements in the discussion about UN-NGO collaboration on security. Indeed, the UN makes it a formal requirement. Various NGO personnel have been sceptical if not outright critical of this. However most of this 'debate' is misplaced because it completely misses the point. Box 13 overleaf offers arguments for a more-nuanced reflection on the issue of staff with a military or police background.

The real questions that a management approach should start from are:

- What range of competences is generally required for safety and security management?
- Does a person understand the differences between major security strategies?
- What range of competencies is required for a general, HQ-based security focal point?
- What specific competencies may have to be prioritised for a security officer depending on the specifics of a field context?

A comprehensive understanding of aid agency security indicates that a very wide range of competences is required. Few individuals are likely to possess them all in equal measure, although it is possible to learn and become confident in many if not most of them. Indeed, the range would encompass such diverse skills as political and social analysis, managing staff , negotiation skills in different cultural environments, technical knowledge about what makes effective armour and an effective blastwall, first aid for landmine victims, driver instruction training, the technical knowledge to install radios, stress management, first-line support to a rape victim and provide leadership

BOX 12: The effectiveness of safety and security documentation

- How complete is it? Reference documents from different agencies on the same topic have very different degrees of detail. Some agencies have reference documents that cover many more topics than others.
- What should be prioritised? Is it a greater priority to develop guidelines on abduction and hostage survival and management, than on landmines or armed robbery, and why?
- What is the quality and appropriateness of the documents? Particularly on hostage situations, sexual aggression/rape and stress, there is a tendency among agencies to copy from other documents, first those concerning such incidents in the Western world, and now probably increasingly from other aid agency documents that are originally based on Western country references. But do Western-country references reflect the circumstances of threats and incidents in the danger areas where agencies work? Should reference materials not be developed more on the basis of analysed incidents and scenarios pertaining to the environment in which they normally work and have to survive?
- For whom are they written? There is particular blurring between guidance for all field-based staff and field-level managers, probably reflecting the fact that until recently security management focused more on 'security awareness' with little clarity and distinction of what constitutes 'security management'. There is also only a beginning of development of reference materials for HQ people with security-related responsibilities. Distance-managing security and crises can be different from field-managing security and crises, and HQ has its own unique role to play, different from field-based managers. In short, training and reference materials should more clearly distinguish between different 'target groups'.
- What scenario aspect do they cover? Full preparedness in risk management would differentiate between preventive measures to try and avoid incidents, incident survival for those caught up in one, immediate incident and crisis management, post-incident management. Quite a few documents are a usually incomplete and non-differentiated mix of all of those.
- How user-friendly are they? This is an area of often major weakness. A pile of paper is unlikely to be actively and productively used by people with already little time to stand back and reflect, and burdened with too much paper. Safety- and security-related documentation has to be centralised in one reference pack. But that by itself is not enough. Operational agencies are not experts in information management, and tend to underestimate the vital importance of editing documents for internal consistency and reduction of repetition, and of good formatting and attractive presentation. Documents have to be made user-friendly.
- How do you ensure that documents are read and understood? Just handing out a pile of documents in no way guarantees that they are understood and will be actively referred to. Asking people to sign a paper that they have 'read and understood' them, may decrease the organisation's liability, but still does not guarantee anything. There is no alternative but to spend time, and work with people through the documentation, and the principles, logic and rationale behind them, to develop some genuine understanding.
- Where to place them: Three practices are currently in vogue: safety and security guidelines are incorporated in a personnel manual, in an emergency response manual or stand separately.

during a chaotic evacuation. Roughly, there are a series of technical skills, but also a whole series of analytical and relational skills that come into play. Most people are stronger on one or the other. Anybody operating as security focal point with an organisation-wide remit based in HQ, will have to develop knowledge and skill about the whole range, as well as learning how to master the rules of the game in that specific organisation, to effect change and improvement.

In a specific context situation, all skills may still be required, but most situations will indicate higher priority for one set of skills over others. This researcher for example has no professional security background, but trained in social sciences, particularly anthropology and politics. That background proved extremely relevant, and highly effective, in managing security in a Somali and an Afghan environment. That skill in manoeuvring and negotiating one's way in a tribal environment proved less appropriate, however, for dealing with the Sri Lankan army officials. It would probably also be less effective in an environment ridden by violent crime, or in a place like Angola, with many more battlefield-related threats. At the same time, well-trained military did often not get very far (to put it mildly) with their traditional approaches in such tribal environments. Rather then than making decisions on what are little more than petty unrefined prejudices about the military, the police but also the so-called 'non-professional in security', sophisticated managers look at what particular competence fits best the priority requirements of different situations.

Scepticism should not be directed at whether someone has a military or police background, but at the adoption of a standard type of approach to each and every type of security situation. This can apply to the approach typically

BOX 13: Military and police backgrounds: all in the same boat?

- There are a lot of ex-military working with NGOs, including faith-based organisations, in a variety of functions. NGOs sometimes have consciously recruited top managers with a security sector background, because of the expertise they thereby were supposed to bring. NGOs have also recruited ex-military or ex-police officers as security focal points; or NGO managers, partially because of that background, happened to become the security focal point, when security started to appear on the agenda. Some ex-military working with NGOs are immediately recognisable as such, because of their style and attitudes, but other NGO staff would not be recognised as ex-security sector if someone didn't tell you. This is important, because style and approach are a key factor.
- It would also be wrong to see 'military' and 'police' as homogeneous entities, which produced only one type of security professional. Someone who has been with the riot police, is likely to have a different style from someone who spent years in community policing, or in homicide investigations. There are significant differences in the training and styles of a Green Beret or a marine, an SAS person, an infantryman or someone from military engineering. So it becomes relevant to ask 'what military', or 'what police background'?

associated with security forces, primarily using a protection (centred on protective procedures and devices) or a deterrence strategy (centred on the threat of sanctions or the use of armed guards). That can be as misplaced as the single-minded or exclusive pursuit of an acceptance strategy, also in contexts of violent and organised crime or battlefield dangers.

But an uncritical predilection for a protection-deterrence approach to security management, shows a narrow and poor understanding of aid agency security management, and can then indeed have all sorts of potentially problematic implications: it may also influence how a security officer thinks about working with the military or with private security companies (also mostly staffed by ex-military and former police) and about armed guards.

Automatically turning towards ex-military and ex-police also reflects a mind-set that sees security as a specialist domain. An unanticipated result can be that this mind-set inhibits the mainstreaming of security management in the wider management structure. Organisations that have moved more quickly to thus embed security in the general management structure, have not felt the need suddenly to throw out all their managers, and replace them with ex-military and ex-police. This helps to demystify the notion of competence in security management as an exclusively specialist domain.

There is another aspect to it: most ex-security professionals acting as security officers in aid agencies are male, suggesting that security management is a 'male thing' and sometimes turning it into a 'macho thing'. Not only interestingly but importantly, at least one agency has also recruited an ex-police woman, while another recruited a woman to be its first security focal point.
Very few organisations apparently have seriously considered giving national staff security-officer responsibilities. Yet there are obviously national staff with either military and technical knowledge or excellent political analysis and negotiation skills. As there are quite a few national staff operating as logisticians already. As agencies often invest certain security-related responsibilities in their logisticians, there must be more experience around than is commonly assumed. There are certainly various concerns in this regard: the risk of divided loyalty, increased risk for such national staff member, but also potential benefits. As part of a team approach, such national staff member can be given circumscribed responsibilities or kept with a low profile in an advisory role, but the idea need not be discarded from the outset. Much will depend on the context and on finding the right person.

5.4.4 Training and staff development

Anybody with first-hand experience of managing programmes in today's complex emergencies knows that humanitarian aid work requires increasingly multi-disciplinary competence in a wide range of knowledge and skill areas, as well as a high degree of professionalism. It is also clear that more often than not, not all required skills and competence are present in a team. Staff development and being a learning organisation remain daunting challenges.

Among the factors that contribute to the state of affairs are:

- The fact that as recently as 15 years ago (the 1984-85 famines in the Horn of Africa) a valid passport and the readiness to get on a plane in 48 hours were often the only requirements to get a job as expatriate with management responsibilities in the field. Members of that generation of aid workers may currently be in senior management positions and the culture of those days may more or less consciously influence the importance (or not) they attach to staff development.
- The wish in some organisations to retain the spirit of voluntarism, which sometimes leads to negative attitudes towards professionalisation.
- The very low returns on investment in staff development given the high rate of staff turnover.

The result is that often learning-by-doing, and learning-on-the-job continue to be a major staff development path. That this means flat learning curves, and especially too

much reinventing of the wheel and repetition of past mistakes is only gradually beginning to be taken more seriously. Nor are questions always asked about how justifiable it is still today to put expatriates in the early stages of their learning curves in charge of national staff, who perhaps also need to learn new skills and ways of working, but who have significant experience. Finally, by the time that staff members have gained extensive knowledge and skill through learning-from-experience, they are burned out, or need more personal and career stability and therefore leave the sector.

So where are we with regard to developing competence in safety and security management? This review yields the following general observations:

- Prior field experience is seen as highly relevant and sometimes sufficient.
- Training courses are the most commonly used formal tool for competence development.
- A number of organisations have availed themselves primarily of external training opportunities.
- A few organisations provide in-house training to staff. That training can be specifically to do with safety and security, or safety and security integrated into broader training curricula.
- Training on safety and security awareness has advanced much more than on security management competence which appears clearly as the current top priority.
- There remains significant scope for sharper analysis and better management planning of training and staff development.

Some critical reflections can help us develop arguments to make informed decisions.

a. Does experience constitute competence?

Field experience of working in danger zones is relevant, and probably a necessary requirement. The question that is not always asked is whether it is also sufficient? Several agencies state that their HoD and HQ managers are competent because they have extensive field experience, which has become an essential requirement for such postholders.

This equation experience equals competence needs to be challenged. Experience by itself does not turn into full competence, unless it is analysed and reflected upon with a more explicit learning purpose. Second, field experience from a world in which there were fewer threats, greater respect for aid organisations and a habit of risk taking may actually be a liability rather than an asset when it comes to security management. Third, many staff with even many years of field experience (fortunately) have not necessarily had first-hand exposure to all types of threat. It is very possible that they have never had to deal with a situation of a colleague having been raped, a death threat to another colleague, an operational office in a besieged city coming under sustained artillery fire or staff being killed in an air-crash. Finally, much learning has been learning-by-doing, in which a good dose of common sense is very helpful, but that does not guarantee that 'the way we did it in the past' is necessarily the best possible way. In short, experience is a very important building block, but needs to be further shaped and moulded into competence.

The review shows that there is awareness that experience by itself may not be enough, but also that competence and skill development in safety and security management (as opposed to awareness raising) is not yet a strongly recognised organisational priority. A consistently identified weakness was the lack of training in security management, and the fact that field- and HQ-level managers did not find the time and/or the motivation, to avail themselves of existing training opportunities.

b. Using external training courses

External training opportunities can be found in the world of the security professionals but now also increasingly in the aid sector. Some aid workers have been through training courses organised by private security companies, whose clientele may be businesspeople and journalists being sent to danger zones. Among the courses on offer are battlefield survival, and kidnap/hostage survival. They may not be fully appropriate for aid organisations. Some of these companies also offer guard training services, including in the field. Some aid organisations have worked with their national military to provide staff with some basics on security, safe driving, telecommunications, perhaps also first aid.

Then there are courses organised by other aid organisations, either specialised in training, or operational agencies whose courses, however, are also open to staff from other agencies. This can be a stand-alone security and communications course of one or two days, or a component in a longer foundation or basics of aid work and project management type of course. Only with the development of the curriculum under OFDA/InterAction auspices, and its subsequent adoption by RedR, did a real security management course become available in and from the aid sector.

The growing demand for that type of course, at field level but also in the North, and feedback from individuals and agencies confirm its appropriateness. Yet there are different agency practices. Some agencies make it a point of trying to send all their expatriate staff going to risk zones on a security course prior to deployment. Others recognise the validity of certain courses, but leave the initiative to go and follow such a course entirely to the individual staff member. Faced with other priorities, very few may avail themselves quickly of the opportunity.

Using (appropriate) external training opportunities can make a lot of sense. Developing and sustaining in-house training is expensive, and there is no need to reinvent the wheel. It is therefore an excellent option for smaller agencies or those with stronger resource constraints. An

important advantage is also that staff from several agencies will find themselves together on such training course, which enriches the contributions from the participants, enhances common understanding and builds bridges between agencies. There remains a problem, however, with a supply that cannot meet the (growing) demand (see Van Brabant, 1999). It would be highly desirable if other training providers, in the North but also in the South, would adopt the available and tested curriculum and develop a course programme. Another question is how to incorporate the externally developed expertise into in-house knowledge? This requires developing a critical mass of staff with knowledge and expertise on safety and security. One tactic to create such critical mass rapidly is to send not one or two but larger numbers of staff on a training course, in a relatively short period of time, or ask a training provider to run one or more courses just for your own staff.

c. In-house/within-the-family training on safety and security

Some NGOs, UN agencies and members of the Red Cross Movement have developed in-house training on safety and security. The organisational experiences and approaches show different scenarios:

- The organisation has no other in-house training but has developed training specifically around safety and security. The first step tends to be a security-awareness course, which ranges between half a day to three days. The next step can be training on security management.
- The organisation has other in-house training, but has developed specialised safety and security training in order to catch up and develop competence in this particular field.
- The organisation has largely integrated safety and security training in the whole scheme of in-house training. Very specialised training on general or specific crisis management, can be temporarily organised, again to catch up, but will then be integrated in the overall training programme.
- A number of organisations that belong to the same family develop important chunks of training together and their staff join in the training courses.

Table 1 helps to visualise these approaches and can be reworked or developed according to individual agency needs.

Here reflection and planning are required around in-house trainers and training of trainer approaches. It is exceptional for an aid organisation to have a dedicated training division. Most of them therefore look for ways of giving certain staff also a training responsibility. The experience indicates that key factors in the relative effectiveness of this approach will be whether staff are (temporarily) released from other duties or not, and whether they can be deployed in a team rather than alone. Lack of time being the most consistent constraint, it is highly unlikely that staff who do not get released from their normal duties will be able to provide much training to their colleagues. That may also apply to a security focal point who, among other things, is also tasked with training. One organisation's approach has been

Table 1: Safety and security training

Specialised training	Mainstreamed training	Specialised training	
General crisis management training Specific crisis management training, eg, kidnapping	**Advanced management training**	**Advanced logistics training**	**Fundraising and financial management training**
Security management training Specific incident management training, eg, rape reponse	**Basic management training**	**Logistics training** watsan construction warehousing telecoms	**Budgeting and budget management**
Incident survival training Basic survival skill training (map and compass reading, basic car repairs, radio repairs, first aid…)			
Security awareness training	**Training on the project cycle and reporting**		**Book-keeping training**
Induction/orientation			

to select field staff - including nationally recruited staff - who volunteered directly to be trained as trainers, after which their managers were asked to release them. After three or four weeks of ToT, they were then deployed to different field settings to run training courses for some months, before returning to their normal posts. They were also deployed in small teams, averaging three people. A team approach is required as there is hardly any single individual who is equally skilled in the many technical, and the analytical and interpersonal aspects of safety and security management, and who is both very competent in the subject matter and a very good trainer. Apart from that, it is very hard on everybody if one individual would run a full four- to five-day training course.

A team approach has the additional advantage that one can bring in better gender balance and wider language skills. Another organisation has mainstreamed safety and security management in its wider training programme, but has a support capacity of a few security focal points at headquarters, one of which can provide additional training capacity.

d. Planning for training

A non-managed approach to training is to leave it entirely up to individual staff to take the initiative to get training. A semi-managed and pragmatic approach is for managers to be alert for training opportunities, and to avail themselves of such, when they arise. A fully proactive management approach would elaborate a training plan. The key questions then are:

- Who needs to be trained on what, and to what level of competence?
- Who needs to be trained on a priority basis, and why?
- How do we create the time for training, how do we fund it?
- Who can do the training?
- How do we incorporate the learning into our daily working practices?
- How do we sustain an improved level of competence?

The first two questions, rather interrelated, seem obvious, and yet are often overlooked for the simple reason that it requires a prior analysis of job responsibilities, skill requirements and contextual needs. That analysis is seldom done, because there is no time for it, and because it would require that people in the human resource department work closely together with operations managers on other than recruitment and disciplinary matters, which is not always the case. Yet it makes sense to ask what it is that everyone needs to know (safety and security awareness; safe driving, first aid, use of radio/satphones; basics of site security and managing guards, basic guidelines on incident survival and reporting; the identity of the organisation; the basic policies, procedures and practices of the organisation with regard to security), and then who needs to know what in more detail and to what level of competence.

First there is the question of what people need to be trained to do, in other words, the question of the training curricula: what should be a common core, and what contextual options. Then there is the question of to what level of competence people need to be trained. There is a tendency among aid agencies to confuse awareness with competence, hence it seems to be assumed that having attended a one-day security awareness course means that a staff member now is competent. Good practice suggests that a distinction be made between levels of competence (awareness, knowledge of good practices) and skill (actually applied good practice in role play and simulations or real-life situations). There is some correlation between training methods and the development of different levels of competence: case studies, role play, practical and simulation exercise have a stronger life and experiential dimension to them than lectures and theory presentation (see Van Brabant, 1999)

The question of who needs to be trained based on priority is a difficult one, for which there may be no easy answer. There are arguments for prioritising people in the field with management responsibilities, because they will ensure that the rest of the staff behaves in safe and secure ways. But there may also be operational contexts where the top priority may be frontline staff - such as drivers, monitors, registration officers, distributors, nurses in outlying health posts - as the most exposed and vulnerable. There are also arguments for rapid training of senior staff in HQ to mobilise stronger overall commitment in the organisation.

The questions of: how do we create the staff time, how do we fund it, who can do it (internal/external/jointly), and how do we incorporate it in our daily working practices (critical mass of trained staff; training fits within wider organisational developments) have been touched upon elsewhere in this section and in the section on funding and finance.

How do we sustain the increased levels of awareness and competence, especially in the face of staff turnover and loss of institutional memory, is an equally important question. It will require a combination of refresher/training for new staff courses, as well as the incorporation of safety and security management in the organisational culture and daily working practices.

e. Is a training course the sole tool for developing competence?

Probably not. People learn in different ways and many learn constantly through whatever they are doing. There is much to be learned from working with competent people, who take the time, in their daily job, to explain the principles and logic that informs their approaches and decisions. There is also much to be learned from observing, listening to others in informal conversations, reading relevant writings, critically reflecting on one's overall programme or project work in a review or evaluation or thorough analysis of incidents. But a major constraint for people in the field and in HQ alike is lack of time. One of

the major advantages of a formal training course might be simply that it gives staff the exceptional luxury of being able to devote time and attention to one subject.

There is also, however, significant evidence of people going through training courses but then not being able to apply and practise what they learned, because they don't have the time or their working environment is not receptive to the insights and skills they have gained. That suggests that sending people on training courses only makes sense if this is part of a wider drive within the organisation or in certain locations to strengthen the overall awareness and competence around safety and security. In short, individual learning has to fit within a wider organisational learning design.

Tools for more individualised learning are gradually being developed. One aid organisation is producing an interactive CD-Rom on security awareness, which staff can work on when it suits them. Development is beginning of an Internet-based Open University, that allows individual distance learning for any staff member with Internet access. In principle, security-related learning and management materials could be made available this way. A major obstacle to and reason for being careful about this, however, is that open access to aid agency security management techniques on the Internet would allow people with malicious intent to learn everything you are learning, which is not desirable.

One comment here seems appropriate with regard to staff turnover. This is a problem that all agencies face. Interestingly, however, there are many aid workers that move between agencies. It is rather surprising that agencies have not yet more fully grasped the need to work together on developing a wider, common, pool of qualified personnel. It would not be too difficult to develop a type of credit system among aid agencies, in collaboration with training organisations and university departments offering MA degrees and shorter courses on humanitarian aid. Completing these courses would represent certain knowledge and skill levels, and would be taken into account when people want to be included in a roster, and in recruitment. It would also provide an incentive for individuals wanting to enter and advance in the aid world, to avail themselves of learning and training opportunities, and may create movement of staff between a smaller number of agencies insisting more on professional qualifications, thereby somewhat increasing the return on investment in staff development.

Chapter 6
Relating to other actors for security management

The analysis of security management at field level indicates a fair degree of objective inter-dependence between agencies concerned with it. A management review like this also makes it clear that there is significant scope for, and important cost-benefits to be had, from much more interagency collaboration. Yet the most emphatic message of aid organisations is their insistence on retaining full autonomy in security management. That is acceptable, and legitimate inasmuch as they have the formal responsibility. But it should not blind people to areas where collaboration is possible and even actively required.

One aid worker commented, 'There is something unique about security that invites us to work together. We need to develop a common concept, a common language, a common training.'

6.1 NGO–NGO relations

There are in practice a variety of more or less formal or informal interactions between NGOs around safety and security, not only at field level, but also between HQs.

6.1.1 NGO relationships with a certain degree of formality: networks, families and alliances

Several organisations belong to networks, families or more formal alliances. These can be of secular organisations such as CARE International, the MSF or the Action against Hunger families or the Save the Children Alliance. It can be faith-based groupings, such as the Lutheran World Federation, CARITAS Internationalis, or the European Partnership of (Christian) Relief Organisations (EPRO). There is also the UN family and the International Federation of Red Cross and Red Crescent Societies. Within such networks, families and groupings, some members will be operational, some will only collect funds and recruit for their operationing partners. By and large members everywhere retain a fairly high degree of autonomy.

Some networks have working groups, often carried by their operational players, which can be asked to develop operational guidelines or policy and policy positions, on behalf of the various participating members. Safety and security can be addressed in such node.

Where safety and security can become more a point of concern and debate in the relationship between members is around secondments and joint operations or joint offices. In principle, the situation should be clear: the responsibility for the safety and security of a staff member lies with the agency that issues the contract. That agency thereby takes on the full legal responsibility, and would deal with everything, including the next of kin, to do with a staff member affected by accident or incident. Where there are joint offices or operations, often there is a designated lead agency, which in principle will be responsible for safety and security. Where security has a strong priority among all, and there is a common understanding and approach, 'security overrides the petty disputes in the family'.

Complications, however, can - and do - arise when the recruiting agency feels that the contracting agency does not have the same concern or may not have the competence to manage adequately the safety and security of the seconded staff member. Where several agencies establish joint offices to run joint operations, differences may crop up because of different thresholds of acceptable risk; over positioning oneself as neutral or not and what that means in practice; over adopting a high or low profile; or over speaking out about abuses. In theory the standards and authority of the lead agency prevail, in practice serious tensions may erupt.

The impression gained is that this is an area that has not yet received much systematic attention in most families. Much of the collaboration within networks so far seems to run on informal understandings. The question can be asked whether there is not a need to formalise basic principles of collaboration and of decision-making in case of serious differences of opinion related to safety and security management.

The UN has avoided this, at least in principle, by granting ultimate authority to UNSECOORD in New York, which nominates the designated official (for security) from among the HoD of the different UN agencies.

6.1.2 Formal project collaboration

The HSPN project involved five agencies which agreed to pilot it, but, in doing so, agreed to share at least security incident information. The question whether this has led to further formal collaborations on safety and security has not been asked. Sharing of agency practice has been taking place between agencies working with People-in-Aid.

6.1.3 Informal exchanges and collaboration

There is also quite a bit of informal contact, exchanges of information, consultation and collaboration going on between agencies, outside family networks. Usually this isbased on a recognition of like-mindedness and the experience of regularly finding themselves working together in the field. On an individual basis, there is also consultation and exchange of information going on between security focal points or security officers based at

HQ, which is not based on family relations or like-mindedness of their agencies, but simply on common interest and personal respect between people working on the same topics.

6.2 UN–NGO relationships

Between UN agencies, a formal arrangement exists around a designated official who reports directly to UNSECOORD, the Office of the UN Security Coordinator, in New York. The DO can bring together the heads of the different UN agencies in a country in a security management team. UNSECOORD can deploy its own field security officers (FSO) on a cost-sharing basis, while individual UN agencies can also deploy FSOs where no UNSECOORD ones are present, or in addition to those. For some years now, the UN has offered a framework Memorandum of Understanding (MoU) to implementing partners, typically NGOs, that would partly formalise their relationship with regard to security. NGOs, or at least those with some competence in security management, by and large have not been happy with the terms of the MoU and several have rejected it.

UN-NGO relationships especially around security are difficult, although it must be said that in times of crisis, there tends to be great solidarity and mutual cooperation. There is interest in some UN organisations to engage in dialogue with NGOs on security management, and in May 2000 a meeting in Geneva under IASC auspices suggested that some such encounters should be organised. A challenge will be to go beyond some strongly held views. Box 14 summarises these.

These perceptions are not pure figments of the imagination. As long as the respective agencies avoid frank discussions

BOX 14: UN–NGO perceptions about each other's security management

Among the difficulties that UN personnel perceive are that:

- NGOs all 'do their own thing', also when it comes to security, rendering futile any attempt at common strategy, common policy or common position.
- NGO heads of delegation as well as staff appear able to present what are in fact personal opinions as 'organisational policies and positions', with of course a sometimes gross lack of consistency between representatives of the same organisation, that are in place simultaneously or successively.
- NGOs sometimes take excessive risks, throwing caution to the wind.
- NGOs sometimes go too far in their fieldcraft in order to get access, paying in cash or kind at checkpoints to get stolen assets back.
- NGOs are excessively opportunistic— not wanting any UN advice as long as all goes well, but appealing for UN help when they are in trouble.
- NGOs are sometimes slow and reluctant to pay for the costs incurred in a UN- organised evacuation.

Among the strengths that NGOs personnel perceive in UN security management are its telecoms and logistical capabilities (esp. WFP and UNHCR) and its better access to and relationship with local authorities.

Among the difficulties that NGO personnel perceive with UN security management are that:

- It is too bureaucratic, sometimes too much driven by liability-concerns;
- It is too centralised, with decisions about movements on another continent dependent on authorisation from New York ('how ridiculous this is becomes clear if you would suggest that the decision of whether someone can go from Manhattan to Long Island needs to be approved in Islamabad').
- It is overly based on a narrow military and technical security concept, emphasising a protection to deterrence approach, to the neglect of an acceptance strategy.
- There are powerful incentives in UN culture against admitting that provocative behaviour of UN staff or staff and management mistakes can have been contributing factors to an incident.
- The UN has failed to integrate security into the management line, so that the advice of field security officers is not infrequently ignored or overruled.
- A high level security phase is maintained because UN staff then get an extra 'danger-bonus'.
- The UN relies too much on the national authorities, even where this is not effective or is counterproductive; or covers up security problems if it is felt this may upset the host government.
- The UN wants NGOs to share security information with them, but does not itself give out information, or when it does, it has been censored so as not to hurt internal sensitivities or those of the host government.
- The proposed MoU on security arrangements obliges an NGO to accept UN management of its security, an authority and responsibility that NGOs refuse to hand over.

about them, and refuse to accept any need for changes in organisational culture and practice on all sides, a more serious and effective collaboration is unlikely to happen.

It also happens that NGOs or government aid administrations second personnel to UN organisations, in which case the same issues as secondments between NGOs can arise.

6.3 Working with local partners

UN agencies, national Red Cross and Red Crescent societies and international NGOs often work with and through local governmental and non-governmental organisations. In the context of security, that relationship has not yet received much focused attention, probably because agencies, understandably, have chosen to improve their own safety and security management before getting involved with that of others.

Among the range of existing practices and principles can be found:

- 'Our security policies do not extend to local partners.'
- 'We cannot send staff from our organisation on field visits to partners elsewhere, or would withdraw our seconded international staff, if we feel that they do not have the competence to assure their safety and security.'
- 'If a local partner cannot or does not want to be neutral, we cannot work with them and will withdraw or go directly operational.'
- 'Ours is a true partnership for development and social justice, we respect their right to speak out about abuses and human rights violations if, together with relief, that is part of their mandate, and will not stop our partnership because of that.'
- 'We already provide them capacity-building support on disaster preparedness and emergency response, and we offer them some training on safety and security, which they can decide to accept or not.'

There is an understandable logic to all of these positions, and in practice much will depend on your own mandate, the quality of the existing partnership, the contextual risks and opportunities, and your own capacities, priorities and competencies.

But the issue is certainly worth thinking through for each given situation. Both sides in the partnership should learn to ask themselves whether, through their programming or any other act of commission or omission, they might be increasing the risk for the other.

6.4 Civilian aid organisations and the military

Whereas several (but not all) of the Western military are eager to have more contact and work more closely with aid organisations, aid organisations in general have been far less eager, although many so far have had difficulty communicating clearly why. In practice, attitudes seem to differ: some agencies have clearly decided to stay at arm's length from the military, others feel that they should cooperate, even if it affects their image. Certainly on the ground, several agencies have used or had to accept military escorts, some have involved the military in some security training, and within the UN arrangements exist under which serving military officers can be seconded to an aid agency.

The current situation seems to be that very few agencies have a policy on relating to the military, that several are going through serious internal debates trying to formulate policy guidelines, while others are not trying to clarify a position, and decide entirely upon a case-by-case basis.

This is not the place to elaborate on the issue, but it is obvious that there is a need to frame questions more precisely, so that we can structure the thinking. Some useful questions to start with seem to be:

- What type of military deployment are we talking about? The national army of the host government, a single-country peacekeeping force (the Indian Peacekeeping Force in Sri Lanka in 1987-1991; the French *Operation Turquoise* in Rwanda in 1994), regional military forces such as NATO or ECOMOG, unarmed military observer missions or UN-sanctioned peace-support operations (or maybe NATO led).
- When do the reservations arise: around deployments in response to natural disasters (floods in Mozambique), around conflict interventions (preventive deployments, consensual peace-keeping deployments, peace-enforcement operations, post-conflict stabilisation and disarmament deployments?).
- Where do the reservations exactly lie: in their being part of the national security establishment and therefore the (domestic) and foreign policy of certain countries; in their getting involved in humanitarian operations, competing with civilian aid agencies, while being much more expensive (but they do have valuable logical assets); in the fact that an association with the military in a particular context or globally may affect the image of neutrality of humanitarian organisations and humanitarian action; in the fact that we do not want to hand over the authority over the security management of our staff (although we do want them to establish the security conditions for aid agencies to work?); any other reason(s) or combinations of the above.

It does not seem very useful to try and pursue an answer to a general question about aid agency-military relationships beyond some basic principles. The development of policy guidelines can be more usefully pursued by asking under what conditions, with whose military and for which particular tasks what form of relationship is possible?

6.5 Aid organisations and private security companies

A rather similar state of affairs, as for the question about relating to the military, seems to characterise the situation here. In practice, many aid organisations have already made use of local or international private security companies. The services provided have included: the provision of unarmed guards; a general or country-specific security management review; and advice on the management of specific threats, particularly on kidnapping and hostage taking. Some agency staff have gone on courses organised by private security companies, including courses on battlefield survival offered also to war journalists. In the past at least, there were instances of aid agencies hiring their security officers from private security companies. There are also private security companies offering services for the protection of displaced populations in camps. Although not exactly private security companies, but sometimes linked to them, commercial de-mining companies have also been hired by humanitarian organisations.

Few agencies seems to have clear policy guidelines on their use. Positions range from: 'in principle we don't use them, although an exception can be made if there is a compelling case, which has to be authorised by headquarters'; to 'in certain places, like Nairobi, they are almost unavoidable and seem to be generally accepted'; to 'this is a free-market economy, is it an issue?'

There are concerns about a global trend towards privatisation of security; about the ethical integrity of a private security company; about the fact that an agency does not want to hand over its security management to outsiders; about the fact that a company providing you with security gets to know quite a lot about you.

There are also some management principles developed by those who use them: do not make a choice based on cost alone but get quality; ensure that they are legally registered and allowed to operate by the government; get local legal advice and have a local lawyer check the draft contract; and explain to them who you are, what your principles are.

At stake are questions of principle, of context, of choice, and of management. These could usefully spelled out, to inform some policy guidelines (see also Van Brabant, 2000: annex 5).

6.6 Embassies

If not enquired about specifically, embassies would probably not even be mentioned when agencies describe how they manage their security in risk countries. Beyond registering their international staff with them, most do not seem to perceive them as a useful resource. Yet practices seem to differ. A common one seems to be a relationship that is limited to registering international staff with the embassy(ies), and counting on one's own embassy or that of another country for practical support in times of acute crisis. In case of a kidnapping or hostage situation, the embassy(ies) gets involved, but one agency felt it its task to tell the embassy what to do and not to do, rather than let the embassy take over the crisis management.

Few agencies indicate that they explicitly expect their HoD to establish good contacts with the embassies. Some do so, but from the funding perspective, they will establish contact with the embassies of their donors. Others will liaise around security with one or a few embassies - not necessarily their own - that are seen as sharp and informed when it comes to security.

Remarkably, embassies were not mentioned as a useful access route to national authorities.

6.7 National authorities

From a formal legal point of view, the national authorities are responsibility for the security of all those on their territory. The UN, as an intergovernmental body, and the ICRC, with a unique status under international law, enjoy certain special privileges and immunities. The status of other aid organisations, and their legal protection, is vaguer, and more through association with, or by extension from the ICRC and UN which are explicitly mentioned in legal agreements. The pursuit of greater security through protection in international legal frameworks is not a strategy adopted by many NGOs. A remarkable exception though was the practice of one, that is actively interested in reinforcing the legal protection of NGO personnel, and is using a self-made laisser-passer document.

Because of the nature of their organisation, UN agencies tend to interact closely with the authorities, and appeal to their responsibility also when it comes to security. NGOs on the whole take a somewhat different approach. In general they wish to have contact with the authorities as with every other important actor on the scene, but they will again strongly insist on their wish to retain their autonomy with regard to security management. Governments however do not always allow aid agencies to manage security the way they want. They can, for example, limit or restrict the licensing of radios. Official security assessments can also be given a spin for political reasons, and the government, certainly when involved in an internal or regional conflict, is not necessarily neutral. Therefore 'you can't equate state authority protection with security'.

Some organisations will take a very contextual view: how closely you relate to the government, nationally and locally, will depend on their sense of responsibility for the security of people, and on their willingness and capacity to provide the aid agency with security. In some cases an agency may want to keep a strong distance, 'but when you give them

responsibility, you must give them full responsibility'. One agency wants to deal not just with local authorities but also with the political authorities, but will aim for 'people high in the hierarchy but low in profile'. Useful facilitators, entry providers and sometimes intermediaries can be national counterparts of international agencies, some of which are governmental administrations such as the Ministry of Health or the Refugee Administration.

Few agencies seem to have guidelines for dealing with national authorities for their managers (see Van Brabant, 2000: ch. 22 for dilemma scenarios).

Table 2: Factors inhibiting and facilitating change

Inhibiting factors	Facilitating factors
• Attitudes at the top: top managers are not committed, too far removed from field realities, do not understand today's requirements of security management; an old-boy network prevents new thinking coming in.	• Attitude at the top: strong commitment; top managers have (recent) field experience, continue to be exposed to field realities; have an appropriate security concept; corporate safety and security policy.
• Organisational culture: - competitive orientation: the incentive system rewards speed, visibility etc. and thereby encourages risk-taking behaviour; - excessive voluntarism: unclear allocation of authority and responsibility, problematic decision-making procedures, relationships with other agencies very personality driven; - self-congratulatory: we highlight our successes, do not want to examine our mistakes and failures; managerial arrogance: 'we know how to do it, we don't have to learn anything'; - bureaucracy: manage your superiors and your career rather than the situation at hand, cover your back; - excessive operationality: everything verbal, nothing in writing, policies are only paperwork;	• Organisational culture: caring organisation (may increase with more women in management positions); learning organisation (centralise incident reports; incident and crisis management analysis); fieldoriented HQ.
• Organisational structure: excessive centralisation but also excessive decentralisation.	• Organisational structure: limited number of management layers between top executive and head of delegation; standing task force or HQ fora where organisational developments on safety and security can be taken forward and monitored; positions where people in HQ (and the field) can stand back from day-to-day management, and be more reflective, analytical and then proactive; security competence developed in the management line; security focal points in advisory roles but with strong influence and reporting to high-level management;
• Not enough independence: too much consideration for the political sensitivities of host and donor governments, not enough flexible money.	• Internal facilitators: dramatic incidents especially death of expatriate; development of a booklet with guidelines or manual that consolidates the experience and thinking in the organisation; an organisational security review; the ability to retain staff; all staff highly safety and security conscious.
• Shortage of expertise, misuse of expertise: lack of training opportunities; not enough competent security people around or salaries too low to attract and retain them; security treated as a 'specialism', outside the management line, people with competence have no influence.	• External facilitators: external pressures (evolving legislation and concerns over liability; concerns over media interest and the need to be seen to be doing something); external opportunities (informal exchanges and collaboration with other agencies; interagency developments of resources and benchmarks; situation experiences that force the agency to clarify its thinking on certain issues like working with the military, armed protection, thresholds of risk and working with local partners.).
• Organisational and team instability: 'change fatigue' in the organisation, high staff turnover, loss of institutional memory.	
• Excessive workloads: no time, competing priorities for managers, absorbed in day-to-day management ('even if it is a priority, we still have five hundred other things to do').	
• Not a priority: staff and managers in low risk areas, lower risk times.	

Chapter 7
Managing change

7.1 Inhibiting and facilitating factors

In only one organisation were there felt to be no real inhibiting factors to strengthen safety and security management: the whole culture of the organisation is pro-security. Significantly, this organisation has been proactively investing in strengthening its safety and security management for almost eight years now, and continues to do so to sustain the level of competence.

Otherwise, there was very strong convergence in factors that were felt to be constraints and those that had been experienced as facilitating the improvement of safety and security management. Table 2 provides an analytical overview.

7.2 Organisational characteristics

A number of general organisational characteristics and their influence on the ability to improve safety and security management were explored. Box 15 summarises the conclusions.

7.2.1 Less-significant factors

The organisations consulted included agencies of very different staff and budget size. Strengths in safety and security management were found in smaller as well as in very large organisations. Large staff numbers may lead to the belief that there are more human resources available to devote to the improvement in safety and security management. The other side of the coin is simply that it means that more staff can be at risk and whose competence must be developed. Similarly, it would be wrong to believe that faith-based organisations would necessarily be less active on safety and security management. There may be those who adopt an attitude that 'everything is in the hands of God', but others will translate their faith into a culture of care for their staff, and a responsibility to do competent work.

BOX 15: General organisational characteristics and safety and security management

The size of the organisation and whether it is faith-based or secular seems to have little influence on how well safety and security are managed.

Working in a network or 'family' context, working with local partners and decentralisation may or may not complicate the efforts to strengthen safety and security, depending on how these characteristics are managed.

The mandate and the funding base, the layers of management and change fatigue are factors that do have a strong influence.

7.2.2 Factors with variable influence

Belonging to a network or alliance of family-type organisations by itself does not seem to make much of a difference. What counts is whether a member is operational or not. Non-operational agencies may be less safety and security conscious or have less competence. The operational members tend to work together. Where there is a shared concern for safety and security, and common approaches to strengthening it, security will override the petty family rivalries and quarrels. Where this is not the case, the management of safety and security may create tensions and disputes between family members.

Whether an organisation works through local partners influences its safety and security management, will depend according to the scenario:

- the international organisation is not operational, its staff will pay visits to the local partner, but it will seldom deploy staff for a longer period of time in the field; here there may be less felt urgency to strengthen one's own security management, and the degree of dependency on the local partner in this regard remains high.
- the international organisation prefers to work through local partners but is prepared to go directly operational when the local partners do not have the capacity to manage security, or are not perceived as sufficiently neutral; here there is a stronger incentive to develop one's own safety and security management, and there will be more first-hand experience available in-house.

Both strong centralisation and strong decentralisation seem problematic. The strong centralisation of operational security management in a headquarters, puts the decision-making in the hands of people too far removed from the context, may cause dangerous delays and reduce the sense of responsibility among field-based managers. By contrast, very strong decentralisation may lead to inconsistencies within the organisation, and misses on the external checks and balances to counter blind spots, danger habituation and loss of the broader picture, that a field perspective often suffers from. Some organisations therefore have delegated many management responsibilities, while retaining for HQ a closer monitoring role and decision-making authority around certain security issues.

The question of decentralisation and delegation also has to be analysed in terms of timing and capacity. Delegating much authority to the field before competence has been developed, is premature. The critical path requires that first competence is built up before authority is delegated. Second, as more and more responsibilities are delegated to the field, its capacity to take on these responsibilities, in terms not only of competence but also of staff numbers, needs to be beefed up - otherwise the organisation simply creates a situation in which it is physically impossible for field staff to manage everything to the desired and required standards.

Regional offices can play a supportive role in safety or security management, or lead to increased complications. If on the one hand they are only an extra management layer, and there is confusion about reporting lines and management authority between them and HQ, the impact will be negative. If on the other hand their management remit is clearly circumscribed, and competence in the form of regional safety and security trainer/adviser is deployed to them, they can play a valuable support role. Still, there remains a need to monitor wider global trends in security and security management across the regions, and the need for a central focal point in HQ to drive the overall organisational efforts to strengthen its safety and security management.

7.2.3 Significant factors

The mandate of an organisation often does have an influence. Organisations whose main mandate and activity is crisis response are fully geared to this, in all departments and among all staff, and also develop a lot of experience from managing crises almost on a day-to-day basis. Those with a relief and development mandate tend more quickly to develop expertise and competence in the emergencies/disasters unit or wing, than elsewhere. Those who used to have primarily a development mandate, and who increasingly were drawn into emergencies work because of the proliferation of crisis situations and donor funding flows, tend to find it difficult to change gear, certainly among staff that have been with the organisation for a long time.

Including a protection/witnessing role in the mandate, or (re-)activating it in one's programme work, also carries potentially increased risk, and requires adaptations to the ways in which safety and security are managed. Obviously human rights work, whether it be monitoring the situation on the ground or investigating alleged crimes, more often than not is a higher-risk mandate.

The nature of funding rather than the overall annual budget, is an important factor. Organisations that are more reliant on institutional donor funding tend to find it more difficult to develop capabilities and competence in safety and security management. Particularly difficult may be funding capacity at HQ level, the pre-positioning of security-related equipment, and paying for a more proactive staff training plan.

Layers of management is another influencing factor. The more layers at HQ, the more distant top management becomes from realities on the ground. The more layers throughout the organisation, the stronger the likelihood of developing a bureaucratic culture, where everything becomes caught up in administrative entanglements, and where people make decisions and pass on information or not, not on the basis of what is required in the given circumstances, but what will please or displease their superiors.

Organisations need to change to remain adapted to a rapidly changing world. But change also has a cost. It creates periods of confusion, loss of motivation and, if changes and restructuring continue without end, creates profound change fatigue among staff (and local partners). All of that can increase the risk, because people are distracted from monitoring their external environment, because reporting lines and management responsibilities become confused and unclear, because there are staff changes with disruptions in teams, a loss of institutional memory and sometimes of certain competences. Change fatigue will also significantly slow down the willingness and pace with which staff can absorb new practices and skills in safety and security management.

7.3 A management plan for change

Very few agencies seem to develop and refer to a management plan for the strengthening of safety and security. This may not be necessary once there is strong organisational awareness and competence. But it may be a useful tool to drive a qualitative jump at crucial moments of earlier organisational development.

A management plan sets out concrete objectives that the organisation wants to achieve within a defined time frame. It sets priorities and becomes the reference for designating responsibilities and allocating staff and financial resources. It will also be the reference for monitoring progress.

A half-hearted management plan is one that is primarily resource driven, for example, if we have US $100,000 for training, therefore we set ourselves some training objectives. A better-quality management plan reviews the existing situation in the organisation and the overall goal that may take some years to reach. It then considers the range of development needs, the relative priorities in terms of urgency but also impact, and the resources available and required.

Developing the management plan is itself an important step in strengthening the organisation, and becomes a team exercise. A team will explore questions like:

- Where are we in the range of aspects of safety and security management?

- What are the various priority needs?
- How can we weigh them against each other: do we prioritise spread/reach by investing in awareness raising of all staff; do we prioritise competence development at structural points by sending all HoD and GEOM to security management training; do we prioritise investments in security equipment; are there critical paths, steps that need to be taken before others can be undertaken; where should we create critical mass; when do we spread ourselves too thinly?
- What approach must we take to create a full-time security adviser post or nominate a senior manager as security focal point (or both?).
- What are the relative advantages and disadvantages of different choices?
- What are the constraints; where are the opportunities?
- Where can we make incremental but meaningful improvements; where do we need more serious investment?
- What might be inhibiting or delaying factors; what facilitating ones?
- What can we do with our in-house capacity; what external resources can we use?
- What can we take over from others with minimal adaptation; what needs more extensive adaptation to our own requirements?
- What can we do together with other agencies?
- Who will be responsible for driving and overseeing overall implementation; when and how do we monitor progress?

The answers will vary by organisation and according to the stage of development of an organisation. There are no easy answers. But some choices will be better in terms of cost effectiveness and impact than others. A management plan also remains a tool: it can be adapted and changed in the course of its implementation, if the situation so warrants.

ANNEX 1
List of agencies consulted

The numbers refer to the number of people consulted per agency.

Action contre la Faim, Paris	3
CAFOD (Caritas UK), London	1
Church World Service, New York	3
Concern USA, New York	1
FAO (Food and Agricultural Organisation of the UN), Rome	2
International Committee of the Red Cross, Geneva	1
International Federation of Red Cross and Red Crescent Societies, Geneva	2
International Rescue Committee, New York	2
Medecins du Monde-France, Paris	2
Medecins sans Frontieres-Belgium, Brussels	2
Medecins sans Frontieres-Holland, Amsterdam	4
Mercy Corps International, Washington office	1
Merlin, London	4
Oxfam GB, Oxford	1
Save the Children Fund-UK, London	1
Seventh Day Adventist Development and Relief Agency (ADRA), international headquarters in Washington	5
Tearfund, London	1
World Food Programme, Rome	8
World Vision, Monrovia (California)	1
UNHCR, Geneva	2
People in Aid project, London	1

In all 20 organisations were consulted, as well as the People-in-Aid project, with 48 people participating in the consultations.

ANNEX 2
Methodology

This report primarily draws on face-to-face interviews and document study, conducted and collected between May and August 2000. A series of questions, intended as an interview guide, were prepared in advance. These were very much inspired by previous work on field-level security management, consolidated in a Field Manual on 'Operational Security Management in Violent Environments' (Van Brabant, 2000). Some insights in organisational practices and documents, gathered during earlier work, were also used.

Agencies generously shared documents with the researcher. These documents have different degrees of confidentiality. None is referenced in an identifiable way in this report, and the decision whether a document can be shared with another organisation or individual remains with the agency.

The research was conceived and presented as a learning exercise. It did not intend to be an evaluation or audit of how well the agencies consulted manage safety and security. The research methodology employed served the learning function but can not be considered sufficiently robust to pretend to be an evaluation. The insights and critical appreciation offered by those consulted on their agency's practices constitute self-reporting. They were not cross-checked with staff in operational settings. Validation therefore lies in the range of consultations across agencies rather than within an agency.

It should also be borne in mind that the round of consultations represents a snap-shot in time. Improvements in the management of safety and security continue. This research wants to insert itself in and support that ongoing process.

The agencies consulted were not selected in order to obtain a representative sample. From the outset it was clear that a number of US and European NGOs would be included. Given the relative interdependence between agencies in the field with regard to security, the Red Cross Movement and UN organisations were also included. The choice of several individual agencies within these broader institutional categories was mostly determined by the fact that the researcher was aware that in recent years they had been making efforts to improve the overall management of safety and security. Some others, however, were included in order to explore how certain organisational characteristics (faith-based; non-operational node in a wider network or alliance; predominantly developmental mandate) might affect safety and security management. There is no implication that agencies not included in the consultation would not have made efforts to improve their overall safety and security management.

The report therefore does not pretend to provide a statistically valid representative overview of the current state of affairs among aid agencies. The author is fairly confident, however, that it presents a fair picture of the state of affairs among the set of agencies that have made serious efforts in the last few years, to strengthen their overall management of safety and security.

Not formally included in the research are governmental aid administrations, several of which directly deploy aid staff in risk areas (the Crown Agents on behalf of DFID, DART teams on behalf of USAID, the Swedish Rescue Teams, the Swiss Disaster Relief corps, ECHO correspondents and monitors, OECD monitors).

ANNEX 3
Security- and safety-related documentation

There is a vast array of security- and safety-related documents in the aid community. The following gives a rough overview of types of documents encountered by the researcher. There are undoubtedly more documents specific to health and safety that were not collected.

1. Policy documents
- Corporate security policy.
- International hostage policy.
- Crisis management policy document.
- Malicious act insurance policy.
- Code of conduct of the (agency) volunteer/ Personal code of conduct.
- Rules of sexual conduct in (agency) programme.

2. Reference/resource documents (mostly for field-based personnel, some for HQ staff)
- Document setting out roles and responsibilities of various posts in the organisation with regard to safety and security, with visual organigram, description of procedures and levels of authority.
- Security adviser job description (corporate).
- Security management responsibilities for heads of office and sub-offices.
- Field safety/security adviser job description.
- Head of delegation/country representative security package.
- Security management check-list.
- A security situation update form.
- Immunities and privileges of UN personnel (short reference document).
- A key manual/reference document of with guidelines for security on mission.
- How to write your local security plan/a template for security plans.
- Safety of humanitarian workers in conflict situations. Briefing sheet.
- Security guidelines for expatriates working in criminal areas.
- Guideline on national personnel management (broad but includes safety and security).
- Orientation for personal security.
- Orientation to vehicular safety and security.
- Instructions for drivers in (agency) humanitarian convoys.
- Employing and managing armed guards.
- Mission readiness and stress management.
- Coping with stress in emergency situations for managers.
- Guidelines for the care of people returning from the field after evacuation and other stressful events.
- Sexual harassment and abuse of power policy and guidelines.
- Rape response handbook .
- Post-exposure preventive treatment. Guidelines for the attending physician in cases of rape.
- Guidelines for prevention and management of abduction events.
- Security Briefing Sheet. Hostage survival.
- Protocol for handling abduction cases.
- Orientation for landmine security.
- Survey format for office security.
- Assembly area survey guide.
- Working with the local media (as part of security management approach).
- Security incident report format.
- Crisis management guidelines (generic).
- A framework for security management.
- Field security officer guidelines.
- Telecoms handbooks (more technical than managerial).
- How to avoid getting AIDS.
- Traveller health guide.
- Prevent accidents guide
- Check-list for pre-departure and in-country arrival briefing/for handover.
- Guidelines on repatriation (of a sick or injured/deceased staff member)

ANNEX 4
Strengthening organisational safety and security management: Guiding questions for a review

I. Strengthening safety and security management

1. What steps has the organisation taken in the last three to five years to improve the overall management of safety and security?

   - What triggered these steps?

2. Does the organisation see itself as legally and morally responsible for the well-being of its staff?

   - All staff?
   - Primarily international staff?

3. Do you distinguish between 'safety' and 'security' conceptually and in the way various risks are practically managed?

   - Why or why not?

4. Do you have doubts about (rapidly) investing in better safety and security management?

   Do any of the following apply?

   'We are not in the emergency or life-saving business.'
   'We haven't had any deaths in the organisation.'
   'Risk is an unavoidable part of our work.'
   'We have been managing risk for decades with existing tools and competences, there is no need for additional or new measures.'

   - What are the assumptions underlying these arguments?
   - Are they supported by the available evidence and analysis?
   - Do you see improved safety and security management as an obstacle to operations, or as a facilitating factor?

5. Who is driving the improvements in safety and security management?:

   - Senior-management, mid-level management, or both?
   - What attitudes toward safety and security management do board members show?
   - Where is there resistance and why?
   - What is the general attitude when it comes to requests for internal resource allocations for safety and security?

II. Management structures

6. Where do you want to locate the security expertise, in HQ and in the field?

- In operational line management?
- In specialist security officers?
- In the management line supported by one or more security advisers?
- Another option?
- What are the respective advantages and disadvantages of each approach?

7. Do you have a designated 'security focal point' in HQ and/or a designated 'health and safety officer'?

- What are their responsibilities?
- Full- or part-time posts?
- Are there in-house stress counsellors?

8. Where in HQ do you locate the security focal point/security officer, the health and safety officer and the stress counsellors?

- In the emergencies/disaster response unit?
- In operations?
- In human resources?

- Is safety and security a major concern for emergencies people only?
- How do you ensure close collaboration between operations, human resources and the policy unit?

9. Who at field level has responsibility for the safety and security of staff (and assets)?

- Does the head of delegation delegate safety and security tasks?
- Does the head of delegation delegate responsibilities?
- Who is responsible in the 'deep field operational bases' outside the capital city?
- Are lines of authority and responsibility clearly defined:
    - For staff members within HQ?
    - In the field?
    - Between HQ and the field?
- Are lines of communication and reporting clear?
- Is it clear how major decisions are made?
- Do you have regional offices between HQ and the country office?
    - If so, what is their role in safety and security management?
    - If so, does their existence blur the lines of authority, communication and the decision-making process?
- Are all managers and staff well informed about allocation of authority/ responsibility and the decision-making process?

III. Management tools

10. Where does discussion about organisational safety and security management take place at HQ?

- Is senior management sufficiently involved?
- Do the mechanisms allow for follow-up of decisions and supervision of their implementation?

11. Did you ever conduct an organisation-wide safety and/or security review?

- What would be the potential advantage of doing (re-doing) one?

12. What do senior and mid-level managers actually understand when they hear 'security' for aid agencies (what comes to mind)?

- Is the concept in people's minds an appropriate one for aid agencies?
- Is there a common understanding?

13. Does distinguishing between an acceptance, a protection and a deterrence strategy for security make sense to you?

- How do you work with these strategies in your security management?

14. Do you have a corporate safety and/or security policy?

- What is in it? Is anything missing?
- Are there advantages/disadvantages of developing one?
- Who should draft it?
- Who should 'sign off' on the final document?

15. What are the current main expenditure lines for safety and for security?

- What new required expenditures do you see coming up in the next two to three years?
- Do staff already habitually write these expenditures into the project and programme budgets?
- Where can spending be made more cost-effective?
- How do/can you fund non-project expenditures?
- How can you retain a reserve or revolving fund of flexible money to respond rapidly to sudden-emerging needs?
- What are the two or three essential requirements you have difficulty funding?
- What discussions do you have with institutional donors for the funding of safety and security expenditures?

16. Do safety and security issues come up in the internal organisational newsletter or magazine?

- If staff are lost in an accident or incident, is there any way in which the organisation can remember and honour them?

IV. Implementing improvements

A. Operational reinforcements

17. Do you habitually carry out a **risk assessment** before going in or returning to a potentially dangerous area?

- Who does it?
- How rigorous is it?
- How competent are your staff at doing risk assessments?
- Does it hinder the need to be there first and fast? Why?

18. Do you see '**neutrality**' **and/or** '**impartiality**' as part of your operational security strategy?

- In what way?
- How in practice do you operationalise this?
- Does it influence what sort of national staff profile you want to recruit in a divided environment?
- How well do your field staff understand 'neutrality' and 'impartiality' in practice?

19. Do all your field offices have a **security plan**?

- Only those in high-risk areas?
- How do you rate their quality?
- Are they actively used?
- How effective are they at reducing risk?
- What checks and balances do you have in HQ to monitor the quality of the risk assessment and of the approaches adopted to reduce risk?
- Is a security plan sufficient? What other important field-level management tools might be required to maintain high standards in safety and security management?

20. Are you confident that all **serious incidents are reported to HQ**?

- Most?
- Not many?
- Only those affecting your agency?
- Those that affected other agencies in the same area of operations?
- Is incident reporting mandatory for field managers, including the narrowly avoided incident ?
- Are incidents documented?
- Do you have a standard incident report form?
- Are the incident reports centralised in the field and in HQ?
- Can they easily be retrieved?
- Are there organisational disincentives against the reporting of incidents?
- How common is it for your organisation to carry out an incident analysis?
- What are the organisational incentives/disincentives with regard to incident analysis?
- Does an incident analysis automatically lead to a review of the security measures at the field level?
- How are the lessons from the analysis of an incident managed, and fed back into organisational policies and practices?
- Do your field managers habitually share incident reports with other organisations in the same context of operations?
- Are they given organisational guidance or directives in this regard?

21. Have you used a form of **armed protection** in any of your field operations?

- Do you have a policy guideline on the use of armed protection?
- Who can decide on the use of armed protection?

22. How important are **telecommunications** in your security management?

- Do you see them as always reducing the risk, or can their presence also increase the risk?
- Can you provide your field offices with the expertise to install and operate radios and satphones correctly and safely?
- Do you feel up-to-date with recent developments in telecommunications?

23. Do you need other technical knowledge, do you have it at hand?

- Can you provide your field offices with the technical knowledge to improve site protection in the face of a rise in crime?
- If you operate also in battlefield zones, can you provide your field offices with the expertise to build bomb shelters and blastwalls correctly, and to give correct advice on the effectiveness of methods to reduce the impact of mine blasts on vehicles?
- Do you need to update yourself on technical aspects of the threat of new weapon deployments and protective measures against them?

24. Have you thought through who at HQ would be core members of a crisis management team?

- Is there clarity about the decision-making process?
- What types of crisis have you prepared for, which ones not?
- Is there clarity about good practice or key attention points in the management of specific types of crises?
- How do crisis managers acquire and refine their competence?
- Do you need to have a 24-hour communications-with-HQ capacity, with duty officers?
- Is the decision-making authority of a duty officer clearly defined?
- Is the hand-over process from one duty officer to the next adequate?
- If you need outside expertise for the management of specific crises, have you identified where you can get it?
- Are you clear how the outside expert(s) will relate to your management authority?

B. The management of specific threats

25. How prepared and competent do you consider yourself to be to manage a case of kidnapping or hostage taking of one or more staff members ?

- *Note*: a policy not to pay ransom is not sufficient 'preparedness'.

26. How well does your organisation acknowledge the risk to your staff of sexual aggression and rape?

- How are you addressing it?
- What are you doing to reduce the risk?
- Do you believe that not deploying or withdrawing female staff from high-risk areas goes against your gender policy?
- Can the security policy be overridden by the gender policy?
- How well prepared are field managers to provide an immediate response and support to sexually assaulted staff?
- Protecting the confidentiality of the victim is a key principle of rape response management. Do you acknowledge that, in certain circumstances, there may also be a need to alert other organisations to the occurrence of such incident and therefore the existence or seriousness of this threat?

27. How proactive is your organisation in creating awareness about and helping to reduce the risk of sexually transmitted diseases?

- Do you make condoms available to all staff in the field? If not, why not?

28. How proactive is your organisation with respect to:

- Improving driving skills and safe driving among staff?
- Managing the risk of fire hazards in offices, residences and warehouses?
- In having first-aid kits available in the field?
- Giving staff the competence to administer first-aid?
- Preparing staff for deployment in difficult environments that carry their own additional risks such as a jungle, desert, mountain area with heavy snowfall, or where travel is often required with local transport with inadequate safety standards?

C. Improving personnel management

29. Do you have war risk and malicious act insurance for your staff?

- For all staff in high risk zones?
- Have you checked the standing exclusion clauses?
- Are you sure there are no contextual exclusion clauses?
- Is the premium in case of disability or death adequate to support dependants?
- Can you negotiate a reduction in the premium when demonstrating improved safety and security management?
- Are you prepared to dip into your own reserves to provide additional financial support to a victim of a safety and security incident, if there is no adequate insurance?
- Are you sure that having staff sign a document that they will not hold the organisation accountable in case of accident or incident is legal and will stand up in court?

30. How are you bringing safety and security management into the whole recruitment/ orientation/assignment cycle?

- How do safety and security come up in the recruitment process?
    - In recruitment of all?
    - Only in certain categories of staff or for certain deployments? Why?
    - Does your recruitment process gauge the attitudes and abilities of candidates?
- Does an emphasis on safety and security work against equal opportunities?
    - How can that be mitigated and overcome?
- Are safety and security addressed in the induction/orientation course?
    - Is the time available and the content presented adequate?
    - How do you ensure that all staff, from wherever they are recruited, get a basic orientation, including on safety and security?
- Do you typically organise a pre-departure briefing for international staff, and does it include the risks and the measures to reduce risk in a given assignment?
    - Are briefings also organised for staff and consultants going on shorter visits?
    - Are field offices expected to provide (further) briefing upon arrival, and do they have the time for it?
    - How do you verify that a briefing took place and was comprehensive?
    - Could a check-list for induction and pre-deployment briefing be useful?
    - And one for hand-over between field managers?
- Can staff at any time in the recruitment and deployment change their mind and withdraw if they feel that the risks are more than they can cope with?
- Which staff members are debriefed upon termination of their contract or their assignment?
    - Is there specific attention to their experience of risk and of the adequacy of the safety and security management?
    - How are the lessons coming out of de-briefings absorbed into organisational practices?
- Is attention paid to their levels of stress?
    - Do you offer staff external counselling and therapy, is it mandatory or not, and why or why not?
    - Does the insurance cover the costs?
    - Is the stress level of a staff member taken into account in decisions about re-deployment? If not, why not?

31. Is it clear what responsibilities of individual staff members are when it comes to safety and security, and what the extent and limitations are of the organisational responsibility? (Including for national staff?)

- Do you inform staff at risk in more detail about what the organisation commits itself to do in cases of ,for example kidnapping, sexual aggression, etc.? If not, why not?
- Are you up-to-date with your legal obligations as an employer for the safety and security of staff?
- Do field offices know the local legislation?
- Are there different legal obligations and liabilities depending on the nature of the contract?
    - Are staff being openly informed about this?
- Is it moral and/or legal to have staff sign a 'waiver' of their right to hold to the employer accountable?
- How much liberty can you allow individuals in refusing to go to or stay in a risk zone?
- Are security rules mandatory and is a breach of them the possible cause of disciplinary action?
- Do you give field staff the message that they represent the organisation 24h/day and 7days/week, and that their personal behaviour is a matter of concern if it affects safety and security and organisational image?
    - Is that expressed in any more formal way, such as a personal code of conduct?
    - How detailed can you be about this?
- Are there or must there be differences when it comes to standards of behaviour of international and of national staff?
    - Are field managers given guidance on how to manage (potential) problems of this nature?

32. Does your organisation acknowledge stress as a health, safety and security issue?

- What practical steps are taken to reduce stress and manage stress levels?
- Do you focus on post-traumatic stress or do you also address cumulative stress?
- How effective are your measures?
- What are the obstacles, how can they be overcome?
- Do you have in-house capacity, in HQ and/or in the field, to provide 'emotional first-aid' or stress counselling?
- Who monitors the stress levels of field managers?

33. Do you have clear moral principles and/or policy guidance to inform your commitment and actions towards the safety and security of national staff?

- How consistent are your actions with your values?
- Do you recognise that the question of security for national staff entails more than just the issue of their evacuation or non-evacuation?
- Do you recognise the need to differentiate between international and national staff members, and within the category of national staff, in a vulnerability to threat assessment?
- Do you recognise the potentially different management responses to for example stress, sexual aggression, kidnapping of national staff members?
- What guidance can you/do you give field managers to proactively identify appropriate responses for national staff members?
- Are you strengthening the awareness among national staff of safety and security issues?
- How can you strengthen their competence?
- Can selected national staff members play an active role in your safety and security management in specific contexts?

D. Competence, knowledge and skill development

34. Have you identified external expertise, external resources (documents, projects) you can use in your own safety and security management?

- What do you need to develop in-house?
- What do you need to adapt for in-house use?

35. Where do you put guidance on safety and security management?

- In a personnel manual or an emergency response manual?
- In separate documents?
- If you put all your safety and security-related documentation together, how complete is it?
- What is the quality?
- How appropriate are the documents and the guidelines?
- For whom are they written?
- Is there a blurring of documents for all staff with documents essentially for managers?
- Are the guidelines and advice limited to prevention, or do they also include incident survival and immediate incident response?
- How user-friendly is the documentation?
- How do you ensure that the documents are read and understood?

36. What range of competencies is required for:

- Safety and security management?
- An HQ-based security focal point (as separate from a health and safety officer)?
- What specific competencies may be required for a security officer in the field?
- Could the specific competencies required in the field vary according to the context?
- Does the fact that somebody has a military or police background (or not), by itself say much about his or her strengths and weaknesses in relation to the competencies required?
    - How useful or essential is such background to qualify for security management?
- Can women be competent in safety and security management or is it a 'male' skill?
- Can you envisage appointing a woman as security adviser or trainer?

37. What mechanism do you or can you use to develop staff competence in safety and security management?

- Does prior field experience by itself guarantee competence?
- Does 'awareness' equal 'knowledge', and does 'knowledge' equal 'skill'?
- How can you quickly create a critical mass of competent staff?
- How important is formal training as a mechanism for staff development?
    - Who needs to be trained on what, and to what level of competence (skill)?
    - Who needs to be trained on a priority basis?
    - When should staff ideally be trained? At what point in their career or their deployment?
    - How can you ensure that people can apply what they learned in training when they return to their training environment?
    - How does training fit within the wider organisational development?
    - Do you need to develop in-house training, or can you rely on outside training opportunities, or take over an existing training curriculum?
    - Is there a need to have separate training events on safety and security? Can it be integrated in existing training events?
- What could be done on an inter-agency basis to increase the pool of aid workers aware of and/or competent in safety and security management?
- Are there other learning methods you could explore or reinforce, such as mentoring on the job, distance learning, interactive learning materials... .?
- How will you sustain the same level of awareness and competence in the face of staff turn-over?

V. RELATING TO OTHER ACTORS FOR SECURITY MANAGEMENT

38. If you are an NGO, do you work with other NGOs on safety and security management?

- How formal or informal is that collaboration?
- Can it be strengthened, broadened?
- If you second staff to another organisation, how do you check that they manage safety and security to proper standards?
- What will you do if you do not feel satisfied that this is the case?
- If you run a joint office or joint operation with another agency, who is responsible for security, and who is accountable?

39. In times of crisis there tends to be great solidarity and cooperation between UN agencies and NGOs but in other times the relationship, when it comes to security management, is difficult.

- What is your perception of the strengths and weaknesses of UN security management?
- What is your perception of the strengths and weaknesses of NGO security management?
- How can a constructive dialogue be developed between the UN and NGOs for better collaboration?

40. If you work with local partners, what commitments and concerns do you have with regard to them when it comes to safety and security?

- To what degree do you rely on their risk assessment and risk management?
- Would you fund safety and security expenditure for them?
- Would you offer them opportunities for awareness and skill-development?
- What can you learn from them about surviving in a particular environment?
- How will you relate to them if they cannot be perceived as 'neutral' or they do not want to be 'neutral'?

41. Have you ever used military protection in one of your field operations?

- Do you have policy guidelines on working with the military with respect to security?
- If there is unease or debate within your organisation, what precisely are the issues and concerns?
- How can these be articulated and thought through, to inform the development of policy guidelines?

42. Have you ever used private security companies for the security of your field operations?

- Do you have policy guidelines on the use of private security companies?
- If there is unease or debate within your organisation, what precisely are the issues and concerns?
- How can these be articulated and thought through, to inform the development of policy guidelines?
- If there are circumstances under which you can accept the use of private security companies, what management guidelines can you usefully offer field staff?

43. Do you relate to your own embassy, or the embassies of other countries, for your security management,?

- To what degree?
- Do you advise your field managers to establish good relationships with their own/other embassies? Why?
- Do you see an embassy as a useful access route to national authorities, if needed?

44. What is your general attitude to the national authorities where it comes to the security of your staff and assets?

- How can you work constructively with the national authorities, without abdicating your own responsibility and management control for the security of your staff and assets?
- What guidance can you give field managers in this regard?

VI. MANAGING CHANGE

45. What are the factors in your organisation that are **inhibiting or delaying progress** in organisation-wide safety and security competence?

- What are the factors in your organisation that are facilitating such progress?

46. Are there general **organisational characteristics** that may play a role in the speed with which you develop or can develop competence in safety and security management?

- Your mandate?
- Your staff size?
- The nature or size of your funding?
- The fact that you work in an alliance or a 'family-network' of organisations?
- The degree of centralisation or decentralisation?
- The fact that you normally work through local partners etc.?

4 Do you have a **management plan** to drive and direct your efforts for the improvement of safety and security management in the organisation?

- Is it essentially resource driven or objective driven?
- Is it based on a good review of the current situation, of priority needs and a cost-impact analysis?

Koenraad Van Brabant
London, Overseas Development Institute
Humanitarian Policy Group, December 2000

ANNEX 5
A profile of organisational good practice

The following profile is offered for consideration. The overview is presented as a profile rather than a list of indicators. The 1997 People-in-Aid Code of Best Practice in the Management and Support of Aid Personnel (see www.peopleinaid.co.uk) contains six indicators to see whether an agency takes all reasonable steps to ensure staff security and well-being. This review suggests that these are valid, but incomplete. Meeting these six indicators would be necessary but not sufficient to effect good organisational safety and security management. As the People-in-Aid code is meant to be used as a tool, a benchmark and not a norm, it is up to individual agencies to see whether they want to add some or more of the indicators presented here, to monitor their organisational progress.

There is, however, an inherent difficulty with indicators. To be useful as a management tool, the number of indicators has to remain limited. Yet it is possible to elaborate indicators as a cascading waterfall: there are higher-level, more general indicators, that can be filled in with lower-level, more detailed and specific indicators. From a management point of view, indicators also have to be measurable. Yet some of the most important things are not easily measurable. To give an example, one can measure whether staff have been given a pre-departure briefing about the risks in their future operating environment, and whether they have been given a copy of the security guidelines. But it is not easy to measure the quality of such briefing, or whether they are competent in risk-reducing behaviour.

With these caveats then, what would an agency look like that manages the safety and security of its staff and assets in a generally competent way?

- All staff, from the top executive to the field-worker are alert to risk and active and responsible in the pursuit of risk-reducing strategies. Risk management encompasses safety and security risks.

- Risk management is seen as an integral part of good programme and good personnel management, and not as in conflict with them.

- Risk management is part of the overall management responsibilities, integrated in the management line, and a regular agenda item in senior management fora. Specialist expertise and advice can be called upon quickly if needed.

- There is clarity about authority, responsibility and lines of communication related to risk management. By and large authority is delegated to those closest to the threat, but there is ongoing quality control and there are organisational checks and balances.

- The organisation monitors legal developments, trends on the ground, technological developments, and efforts to create new tools and resources, and responds to significant changes.

- A corporate safety and security policy articulates key principles of commitment of the organisation, in relationship to its staff and assets, and to external actors. It is clear how the safety and security policy relate to other policies, such as a gender or equal opportunities policy. The extent of the organisation's practical and financial commitment to different types of staff and for specific types of incident and consequences thereof, is also made clear.

- The organisation provides adequate insurance cover to staff, with extended cover for staff in higher-risk areas.

- All staff members are aware of their individual freedom, but also their responsibilities and obligations with regard to safety and security management.

- Field staff understand the logic behind mandatory security measures, but are also sufficiently contextually knowledgeable to be able to make proper situational judgements.

- Field managers have guiding principles to help determine their relationship to various other actors, notably, the national authorities, embassies, other aid agencies, and military forces, with regard to security management. As a matter of principle, field staff collaborate with others about safety and security, except where this would increase risk or reduce the ability of the agency to take its own decisions.

- Donors and field managers routinely discuss the capacities for safety and security management with their (potential) implementing partners.
- Adequate financial resources are allocated for the development and maintenance of safety and security standards and related competence, and safety and security are routine budgeted into programme budgets.
- Deployment and programme choice and programme design decisions are based on ongoing risk assessment.
- Safety and security are routinely addressed in all phases of the assignment cycle.
- Safety and security related documentation is centralised, easily accessible and presented in a user-friendly way. Staff have a common language and common concepts with which to discuss safety and security.
- The organisational efforts and investments in competence development are directed by a plan, based on a prior analysis of requirements, priorities, critical paths, and multiplier effects. Judicious use is made of external resources to speed up the in-house development of competence.
- Staff are clear about what incidents need to be reported and how, and the analysis of serious incidents is routine practice. The organisation keeps records of incidents and accidents, and this analysis is drawn upon for organisational learning.

ANNEX 6
References in the text

Bertini, C. 2000: Statement by the Executive Director of WFP at the UN Security Council Open Debate on Security of UN Humanitarian and Associated Personnel (www.wfp.org/oed/ed/UNsecuritycoun.htm).

Davidson, S. and J. Neal 1998: Under Cover? Insurance for aid workers. London, People-in-Aid (www.peopleinaid.co.uk/undercover.htm).

Inspection and Evaluation Service 1997: Staff Stress and Security. A management challenge for UNHCR. Geneva, UNHCR.

Jensen, S.B. 1999: Taking Care of the Care-takers under War-Conditions. Who cares? Copenhagen, European University Center for Mental Health and Human Rights (on Alertnet).

Macnair, R. 1995: Room for Improvement. The management and support of relief and development workers. London, Relief and Rehabilitation Network, *Network Paper No. 10* (www.odihpn.org.uk).

People-in-Aid 1997: People in Aid Code of Best Practice in the Management and Support of Aid Personnel. London, People-in-Aid (www.peopleinaid.co.uk).

People-in-Aid 1999: Measure for Measure. London, People-in-Aid (www.peopleinaid.co.uk).

Salama, P. 1999: The Psychological Health of Relief Workers. Some practical suggestions. London, Relief and Rehabilitation Network, *Newsletter 15* (www.odihpn.org.uk).

Sheik, M. et al. 2000: Deaths among Humanitarian Workers 1985-1998. Baltimore, Johns Hopkins School of Hygiene and Public Health (contact Gilbert Burnham at gburnham@jhsph.edu).

Slim, H. and I. McConnan 1998: A Swiss Prince, A Glass Slipper and the Feet of 15 British Aid Agencies. London, Disasters Emergency Committee.

United Nations 2000: Safety and Security of United Nations Personnel. Report of the Secretary-General. New York, UN, General Assembly (18 October 2000).

Van Brabant, K. 1997: Security Guidelines. No guarantee for security. London, Overseas Development Institute, Relief and Rehabilitation Network, Newsletter No. 7 (www.odihpn.org.uk).

Van Brabant, K. 1998a: Security and Humanitarian Space - perspective of an aid agency. Bochum, Humanitares Volkerrecht (1):14-24 (www.odi.org.uk/hpg, see under publications, Van Brabant).

Van Brabant, K. 1998b: Cool Ground for Aid Workers. Towards better security management in aid agencies. *Disasters* (22) 2:109-25.

Van Brabant, K. 1999: Security Training. Where are we now? London, Overseas Development Institute, Relief and Rehabilitation Network, discussion paper (www.odihpn.org.uk).

Van Brabant, K. 2000: Operational Security Management in Violent Environments. A field manual for aid agencies. London, Overseas Development Institute, Humanitarian Practice Network, Good Practice Review No. 8 (www.odihpn.org.uk).

World Health Organisation 1998: Occupational Health of Field Personnel in Complex Emergencies. Report of a pilot study. Geneva, WHO, Division of Emergency and Humanitarian Action/ International Centre for Migration and Health.

ISBN 0-85003-494-9

Overseas Development Institute

111 Westminster Bridge Road
London
SE1 7JD

Tel: +44 (0) 20 7922 0300
Fax: +44 (0) 20 7922 0399

Email: publications@odi.org.uk
ISBN: 0-85003-494-9 £8.00